BAB II

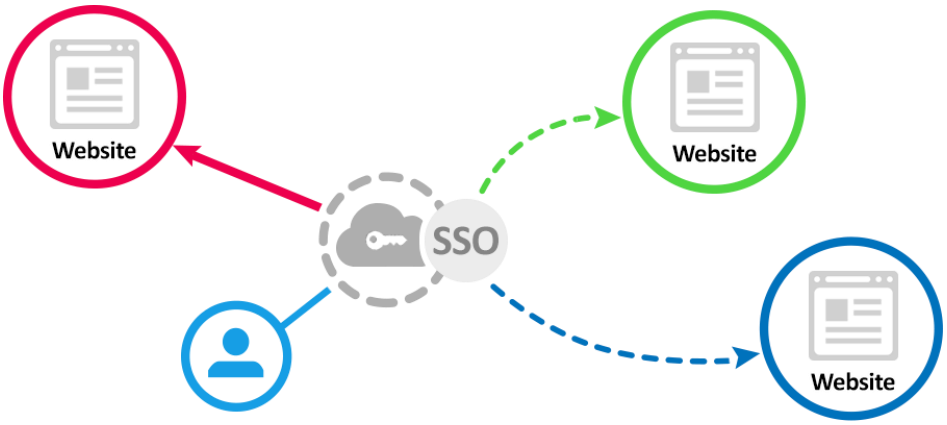
LANDASAN TEORI

2.1 Website

Website atau situs dapat diartikan sebagai kumpulan halaman yang menampilkan informasi data teks, data gambar diam atau gerak, data animasi, suara, video dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink*). Bersifat statis apabila isi informasi *website* tetap, jarang berubah, dan isi informasinya searah hanya dari pemilik *website*. Bersifat dinamis apabila isi informasi *website* selalu berubah-ubah, dan isi informasinya interaktif dua arah berasal dari pemilik serta pengguna *website* (Hartono, 2013).

2.2 Single Sign-On (SSO)

Single Sign On (disingkat menjadi SSO) adalah sistem yang mengizinkan pengguna agar dapat mengakses seluruh sumber daya dalam jaringan hanya dengan menggunakan satu *credential* saja. Sistem ini tidak memerlukan interaksi yang manual, sehingga memungkinkan pengguna melakukan proses sekali login untuk mengakses seluruh layanan aplikasi tanpa berulang kali mengetikan password-nya. (Malang, n.d.)(Aini et al., 2018)(Musliyana et al., 2016). Pada gambar 2.1 merupakan konsep dari SSO.



Gambar 2.1 Konsep *Single Sign On*

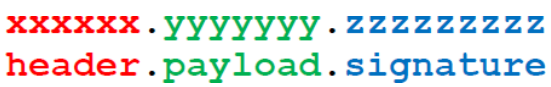
(sumber https://penguinstunnel.blogspot.com)

Konsep SSO ini, sangat diminati dalam jaringan yang sangat besar dan bersifat heterogen, dimana sistem operasi serta aplikasi yang digunakan berasal dari banyak vendor, dan pengguna diminta untuk mengisi informasi dirinya ke dalam setiap multi-platform yang hendak diakses. SSO mengotentikasi pengguna pada semua aplikasi yang telah di authorized untuk diakses. Ini menghilangkan permintaan authentication lagi ketika pengguna mengganti aplikasi selama *session* berlaku (Rudy, 2009).

2.3 JSON *Web Token* (JWT)

JSON Web Token (JWT) merupakan sebuah token berbentuk string panjang yang sangat random yang gunanya sendiri untuk melakukan sistem Autentikasi dan Pertukaran Informasi. Pada umumnya JWT digunakan untuk melakukan login pada aplikasi *website* biasa dimana kita menggunakan *session* untuk mengingat siapa yang sedang *Login*. Berdasarkan JWT, peran pengguna juga dapat dikontrol pada SSO, ini umumnya diperlukan oleh sistem informasi berbasis web untuk

mengelola izin halaman atau fitur yang diberikan kepada pengguna(Putra et al., 2018). JWT tidak bergantung pada bahasa program tertentu. Struktur JWT terdiri atas tiga bagian yang dipisahkan oleh titik (“.”), yaitu header, payload, dan signature (Rahmatulloh et al., 2018), seperti ditunjukkan pada gambar 2.2.



Gambar 2.2 Konsep Struktur JWT

2.4 Sistem Informasi Akademik

Sistem Informasi Akademik merupakan sistem yang memberikan layanan informasi yang berupa data dalam hal yang berhubungan dengan akademik. Dimana dalam hal ini pelayanan yang diberikan yaitu seperti: penyimpanan data untuk siswa, penentuan kelas, penentuan jadwal pelajaran, pembuatan jadwal mengajar, pembagian wali kelas, proses penilaian(Howel et al., 2017).

Menurut (Santoso, 2007) dalam penelitian marisa Sistem Manajemen kademik (SIA) adalah perangkat lunak yang digunakan untuk menyajikan informasi dan menata administrasi yang berhubungan dengan kegiatan akademis. Dengan penggunaan perangkat lunak seperti ini diharapkan kegiatan administrasi akademis dapat dikelola dengan baik dan informasi yang diperlukan dapat diperoleh dengan mudah dan cepat(Marisa, 2019).

2.5 E-Leraning

E-learning merupakan suatu teknologi informasi dan komunikasi untuk mengaktifkan siswa untuk belajar kapanpun dan dimanapun. Pembelajaran elektronik atau *e-learning* telah dimulai pada tahun 1970-an(Hartanto, 2016).

Literatur lain menyatakan bahwa istilah *e-learning* banyak memiliki arti karena bermacam penggunaan elearning saat ini. Tapi pada dasarnya, *e-learning* memiliki dua tipe yaitu *synchronous* dan *asynchronous*. *Synchronous* berarti pada waktu yang sama. Proses pembelajaran terjadi pada saat yang sama antara pendidik dan peserta didik. Hal ini memungkinkan interaksi langsung antara pendidik dan peserta didik secara *online*. Dalam pelaksanaan, *synchronous training* mengharuskan pendidik dan peserta didik mengakses internet secara bersamaan. Synchronous training sering juga disebut sebagai virtual classroom.

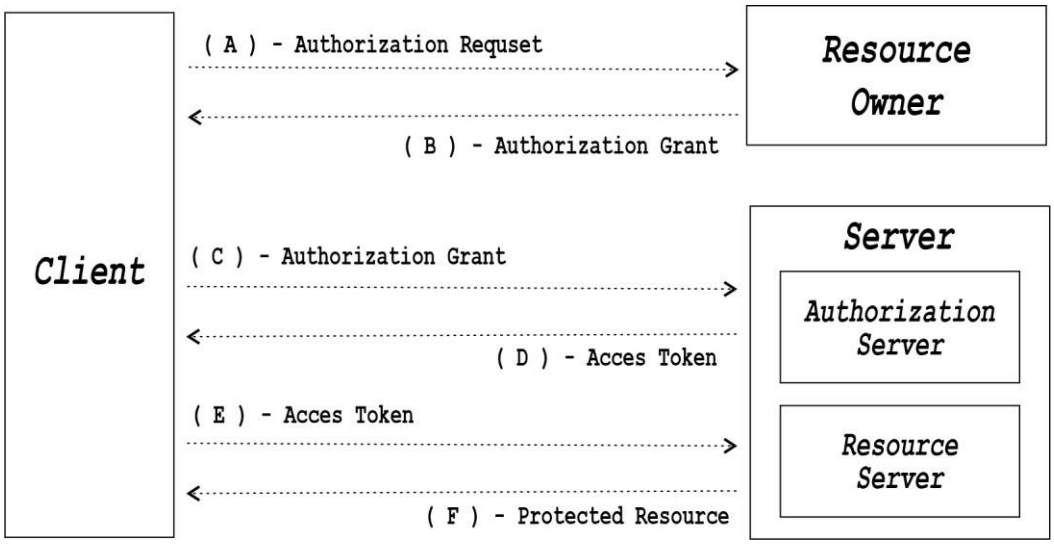
Asynchronous berarti tidak pada waktu bersamaan. Peserta didik dapat mengambil waktu pembelajaran berbeda dengan pendidik memberikan materi. *Asynchronous* training popular dalam *e-learning* karena peserta didik dapat mengakses materi pembelajaran dimanapun dan kapanpun. Peserta didik dapat melaksanakan pembelajaran dan menyelesaikannya setiap saat sesuai rentang jadwal yang sudah ditentukan. Pembelajaran dapat berbentuk bacaan, animasi, simulasi, permainan edukatif, tes, quis dan pengumpulan tugas.

2.6 Moodle

Moodle adalah *platform* bersifat *web-based* yang biasa digunakan untuk keperluan *e-learning*. Dengan kata lain, Moodle dibuat khusus sebagai sebuah sistem manajemen pembelajaran *online* yang efektif. Kepanjangan dari Moodle sendiri merupakan *Modular Object-Oriented Dynamic Learning Environment*. Artinya, platform ini dikhususkan untuk membuat lingkungan belajar online yang dinamis(Vickry Pratama A et al., 2013).

2.7 OAuth2

OAuth2 merupakan suatu protokol terbuka yang mengizinkan otorisasi secara aman dengan metode yang sederhana dan standar dari aplikasi *web*, *mobile* dan *desktop*. Protokol otorisasi OAuth memungkinkan pihak ketiga (third-party) untuk dapat mengakses sumber daya dengan akses tertentu melalui protokol *HTTP*. OAuth dirancang khusus untuk mengatasi permasalahan klasik pada model autentikasi pada *client-server*. Mekanisme kerja OAuth2 terbentuk dari peran aktif 4 (empat) bagian yang terdiri dari : client, resource owner, authorization server, resource server(Fatman, 2020). Berikut pada gambar 2.3 penjelasan proses kinerja Oauth2.



Gambar 2.3 Proses Kinerja Oauth2

Pada Tabel 2.1 merupakan Penjelasan untuk tugas dan fungsi dari komponen – komponen OAuth2.

Tabel 2.1 Penjelasan Kinerja OAuth2

Kode	Keterangan
A	*Client* meminta otorisasi kepada *resource owner*. Permintaan tersebut berupa data *credential* dari *resource owner*
B	*Client* mendapatkan data *credential* sehingga mendapatkan otorisasi kepemilikan *client.*
C	*Client* meminta akses token pada *authorization server*
D	*authorization server* memproses otentikasi *client.* Jika hasilnya valid maka *client* akan diberikan akses token.
E	*Client* meminta *resource* kepada server dengan akses token.
F	*Resource server* akan melakukan validasi *token*, jika valid akan diberikan resource atau suberdaya yang diminta oleh *client*

2.8 Postman

Postman adalah sebuah aplikasi yang berfungsi sebagai *REST CLIENT* untuk uji coba *REST API*. Postman biasa digunakan oleh developer pembuat API sebagai tools untuk menguji API yang telah dibuat. Selain itu, pada penelitian ini postman digunakan sebagai penguji keamanan untuk memvalidasi *token* yang da dapatkan oleh *client*, sehingga proses otorisasi dari sistem akademik dan *e-learning* bisa dilihat dari pengujian tersebut(Anwar & Tjahjanto, 2021).

2.9 Wireshark

Wireshark merupakan suatu tools yang digunakan untuk melakukan analisis dan pemecah masalah jaringan. Hal ini memungkinkan dapat dimanfaatkan untuk untuk mengetahui masalah yang terjadi pada jaringan. Pada penelitian ini, Wireshark digunakan untuk melihat *traffic* jaringan untuk melihat proses otorisasi

dan otentifikasi pada sistem akademik dan *e-learning* atau data yang di kirim oleh *server* ke *client* bisa teridentifikasi.

2.10 Kajian Penelitian Terkait

Berikut merupakan kajian penelitian yang berhubungan dengan *Single Sign On* dan *JSON Web Token* (JWT) dalam autentifikasi suatu sistem atau aplikasi. Berikut pada tabel 2.2 merupakan tabel terkait penelitian yang akan dilakukan.

Tabel 2.2 Kajian Penelitian Terkait

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
1	Pedro Mestre, Member, IAENG, Rui Madureira, Pedro Melo-Pinto, and Carlos Serodio, Member, IAENG	2018	Multiple JSON Web Tokens for Mobile Distributed Applications	Sistem Multiple JSON Web Tokens untuk aplikasi mobile layak untuk menggunakan sistem tersebut, karena dapat meningkatkan keamanan untuk layanan web dan meniningkatkan kompleksitan aplikasi.(Mestre et al., 2018)
2	I Putu Arie Pratama, Linawati, Nyoman Putra Sastra	2018	Token-based Single Sign-on with JWT as Information Sistem Dashboard for Government	Single Sign-On (SSO) menggunakan Json Web Token (JWT) dalam arsitektur SSO tokenbased dapat diterapkan pada dashboard sistem informasi pemerintah yang menyediakan layanan otentikasi terpusat dan daftar sistem informasi resmi kepada Pengguna (Pratama et al., 2018).

Tabel 2.2 Kajian Penelitian Terkait (Lanjutan 1)

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
3	Aminudin	2014	Implementasi Single Sign On (SSO) Untuk Mendukung Interoperabilitas Aplikasi E-Commerce Menggunakan Protocol Oauth	Single Sign On Sistem dengan memanfaatkan protokol OAuth merupakan teknologi autentikasi dengan kode token sebagai pengganti username & password(Malang, n.d.).
4	Guntoro, Muhammad Fikri	2018	Perancangan Aplikasi Single Sign-On (SSO) Menggunakan Otentikasi Gambar	Perancangan sistem single sign-on (SSO) dengan menggunakan autentikasi gambar memungkinkan bagi pengguna hanya sekali melakukan otentikasi ke dalam beberapa aplikasi web(Guntoro & Fikri, 2018).
5	Yenni Fatman, Renova Octaviawati	2020	Implementasi Metode Open Authorization (OAuth2) Untuk Pengelolaan Data Dosen di Universitas Islam Nusantara	Penelitian menghasilkan sistem yang dapat memberikan layanan dengan kemudahan dan keamanan yang terjamin dalam bentuk modul berbasis Application Programming Interface (API) dengan mengimplementasikan otorisasi OAuth 2.0 dan SMTP(Fatman, 2020).
6	R. Sandhika Galih A. & Faerul Salamun2	2018	Implementasi Web Service pada Aplikasi Mobile untuk Mendukung Sistem Informasi di Bandung N-Max Community	Implementasi Web Service pada sistem ini bisa mengoptimalkan sistem informasi N-Max community(Salamun et al., 2018).

Tabel 2.2 Kajian Penelitian Terkait (Lanjutan 2)

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
7	Alam Rahmatulloh1, Heni Sulastri2, Rizal Nugroho	2018	Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512	Penerapan algoritme HMAC SHA-512 pada JWT dalam WS dan pada arsitektur 64-bit menghasilkan kinerja yang lebih baik. SHA512 lebih cepat 1% dibandingkan dengan SHA-256(Rahmatulloh et al., 2018).
8	Rohmat Gunawan, Alam Rahmatulloh	2019	JSON Web Token (JWT) untuk Authentication pada Interoperabilitas Arsitektur berbasis RESTful Web Service	otentikasi berbasis token menggunakan JSON Web Token telah berhasil diterapkan pada layanan web danbackend sistem blood donors. Sehingga layanan web ini mampu mengatasi permasalahan interoperabilitas(Gunawan & Rahmatulloh, 2019).
9	Zuhar Musliyana, Teuku Yuliar Arif, dan Rizal Munadi	2016	Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia	Penerapan algoritma Onetime Password dengan kombinasi Salt pada pengecekan sesi_id user SSO dapat menanggulangi kemungkinan aksi intercept terhadap penyalahgunaan hak akses user(Musliyana et al., 2016).
10	Obinna Ethelbert, Faraz Fatemi Moghaddam, Philipp Wieder, Ramin Yahyapour	2017	A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications	Implementasi fitur stateless dan JWT untuk autentikasi dan akses otorisasi untuk pengguna cloud mampu menjadwab keamanan dan privasi komputasi cloud SaaS(Ethelbert et al., 2017).

Tabel 2.2 Kajian Penelitian Terkait (Lanjutan 3)

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
11	Yesi Novaria Kunang, Ilman Zuhri Yadi	2014	Sistem Single Sign On Universitas Berbasis Cas-Ldap	Sistem Single Sign On ini sangat memungkinkan diimplementasikan pada Universitas berdasarkan hasil sementara yang sudah diujikan pada server SSO berbasis CAS yang digunakan untuk mengintegrasikan layanan elearning, email dan blog. Dari sisi keamanan sistem SSO yang dikembangkan cukup aman terutama dengan penggunaan https dan fitur ldap over TLS sehingga komunikasinya terenkripsi. Dengan demikian tidak bisa dilakukan proses sniffing data dan password oleh hacker(Kunang & Yadi, 2014).
12	Andri Warda Pratama Putra, Adhitya Bhawiyuga, Mahendra Data	2018	Implementasi Autentikasi JSON Web Token (JWT) Sebagai Mekanisme Autentikasi Protokol MQTT Pada Perangkat NodeMCU	Pengujian dari implementasi autentikasi JWT dengan menggunakan NodeMCU dengan 3 pengujian yang dilakukan diperoleh hasil bahwa server yang diimplementasikan dengan menggunakan framework Node.js dapat melakukan autentikasi terhadap token yang dikirimkan oleh publisher(Putra et al., 2018).

Tabel 2.2 Kajian Penelitian Terkait (Lanjutan 4)

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
13	Bagus Satria, Ari Kusyanti, Widhi Yahya	2018	Implementasi Algoritme Blake2s pada JSON Web Token (JWT) sebagai Algoritme Hashing untuk Mekanisme Autentikasi Layanan REST-API	Implementasi algoritme BLAKE2S pada library JSON Web Token berhasil dilakukan dengan menambahkan pilihan untuk menggunakan algoritme BLAKE2S pada JSON Web Signature (JWS) dan algoritme BLAKE2S disertakan pada konfigurasi JSON Web Algorithm (JWA). Algoritme BLAKE2S memiliki waktu ratarata autentikasi 88,583 ms(Satria et al., 2018).
14	Qurotul Aini, Untung Rahardja, Romzi Syauqi Naufal	2018	Application Single Sign On with Google the Website Based on Yii Framework	Pengimplementasian metode Single Sign On (SSO) pada website yang menggunakan yii framework dimana pengguna web service berbasis yii framework terbantu dengan diimplementasikan Single Sign On bisa mempermudah mahasiswa karena tidak perlu menggunakan banyak account(Aini et al., 2018).

Tabel 2.2 Kajian Penelitian Terkait (Lanjutan 5)

NO	PENELITI	TAHUN	JUDUL	HASIL PENELITIAN
15	Irfan Darmawana, Alam Rahmatulloh, Rianto, Ilman Hilmi Orizab	2020	Authentication System and Method for Improving Security Login without Typing Password	Penelitian ini membahas tentang otentikasi login proses yang dapat melakukan integrasi login tanpa mengetik kata sandi, karena kata sandi dihasilkan berulang kali dengan One Metode Time Password (OTP), dan menggunakan Quick Response Code (QR) sebagai pendukungnya(Darmawan et al., 2020).

2.11 State of The Art

State of the art dilakukan untuk menjelaskan letak perbedaan dan keterbaruan yang ada pada penelitian yang sedang dilakukan, dan melihat korelasinya dengan penelitian sebelumnya yang terkait diantaranya adalah impelementasi dari *Single Sign On* dengan beberapa cara untuk otentifikasi pada sistem yang diterapkan. Berikut pada tabel 2.3 merupakan persamaan dan perbedaan dengan beberapat penelitian terkait *Single Sign On* (SSO).

Tabel 2.3 Persamaan dan Perbedaan dengan Penelitian Terkait

No.	Nama Penulis, Tahun, dan Judul	Hasil Penelitian	Persamaan	Perbedaan	
				Penelitian Terdahulu	Rencana Penelitian
1.	I Putu Arie Pratama, Linawati, Nyoman Putra Sastra. (2018). *Token-based Single Sign-on with JWT as Information System Dashboard for Government*	- Implementasi *single sign-on (SSO)* dengan menggunakan otentifikasi JWT padasistem pemerintahan .	- Implementasi konsep *Single Sign On (SSO)* - Penggunaan otentifikasi akun menggunakan JWT	- Implemntasi dari perancangan *Single Sign On (SSO)*, untuk sistem pemerintahan	- Implementasi perancangan *Single Sign On (SSO)*, pada sistem akademik pesantren dan *Elearning*
2.	Qurotul Aini, Untung Rahardja, Romzi Syauqi Naufal. (2018). Penerapan *Single Sign On* dengan Google pada Website berbasis YII Framework	- Implementasi metode *Single Sign On* (SSO) dengan Google pada *website* yang menggunakan yii framework bisa mempermudah mahasiswa karena tidak perlu menggunakan banyak account.	- Implementasi konsep *Single Sign On (SSO)*	- *Single Sign On* menggunakan Google	- *Single Sign On* menggunakan API sendiri.

Tabel 2.3 Persamaan dan Perbedaan dengan Penelitian Terkait (Lanjutan 1)

No.	Nama Penulis, Tahun, dan Judul	Hasil Penelitian	Persamaan	Perbedaan	
				Penelitian Terdahulu	Rencana Penelitian
3.	Guntoro, Muhammad Fikri. (2018). Perancangan Aplikasi *Single Sign-On (SSO)* Menggunakan Otentikasi Gambar	- Perancangan sistem *single sign-on (SSO)* dengan menggunakan autentikasi gambar	- Implementasi konsep *Single Sign On (SSO)*	- Implemntasi dari perancangan *Single Sign On (SSO)*, tidak ada keamanan yang diuji pada sistem tersbut.	- Otentifikasi menggunakan menggunakan token dan dilakukan pengujian keamanan.
4.	Aminudin. (2015). Implementasi *Single Sign On* (SSO) Untuk Mendukung Interoperabilitas Aplikasi E-Commerce enggunakan Protocol Oauth	- Implementasi SSO untuk mengotentikasi aplikasi *e-commerce* dengan menggunakan penyedia *account* yang mendukung protokol OAuth.	- Implementasi konsep *Single Sign On (SSO)* - Menggunakan protokol Oauth	- *login* menggunakan akun media sosial - menggunakan *protocol* Oauth	- *Login* menggunakan username dan password - Menggunakan *protocol* Oauth2