Penerapan Teknologi Single Sign On (SSO) dengan Metode JSON Web Token untuk Meningkatkan Kemudahan Akses Pengguna

Vidya Meidita[#*1], Samsul Arifin [#2], Dian Wahyuningsih [#3], Dinny Wahyu Widarti [#4]
[#1234]Teknologi Informasi, STMIK PPKIA Pradnya Paramita, Indonesia
Korespodensi author *vidyameidita@gmail.com

Info Artikel

Diajukan: 10 Juni 2026
Diterima: 19 Juni 2026
Diterbitkan: 1 Juli 2026

Keywords:
Single Sign-On; JSON Web Token; Access Efficiency; Session Tracking; Token Authentication

Kata Kunci:
Single Sign-On; JSON Web Token; Efisiensi Akses; Pelacakan Sesi; Otentikasi Token

Abstract

This study implements Single Sign-On (SSO) technology using the JSON Web Token (JWT) method at VINSCODE, a software house, to address user difficulties in managing multiple accounts and passwords. The research aims to improve access efficiency and reduce account security risks by integrating JWT into the SSO system. Functional testing, usability testing, and user questionnaires were conducted to measure the system's performance across three indicators: ease of access, logging and tracking, and data security. The results show that users can log in once and move between integrated websites without re-authentication, with all activities accurately logged. Security is enhanced through a verification code sent to users during the first login from a new device. Questionnaire results indicate a high user satisfaction rate, with an average score of 85%, showing improvements in login convenience, account management, and system monitoring. The implementation has proven effective in increasing access efficiency and ensuring secure user authentication across applications.

Abstrak

Penelitian ini menerapkan teknologi Single Sign-On (SSO) menggunakan metode JSON Web Token (JWT) di VINSCODE, sebuah perusahaan pengembangan perangkat lunak, untuk mengatasi kesulitan pengguna dalam mengelola beberapa akun dan kata sandi. Penelitian ini bertujuan untuk meningkatkan efisiensi akses dan mengurangi risiko keamanan akun dengan mengintegrasikan JWT ke dalam sistem SSO. Uji fungsional, uji kegunaan, dan kuesioner pengguna dilakukan untuk mengukur kinerja sistem berdasarkan tiga indikator: kemudahan akses, pencatatan dan pelacakan, serta keamanan data. Hasil menunjukkan bahwa pengguna dapat login sekali dan berpindah antar situs web terintegrasi tanpa perlu otentikasi ulang, dengan semua aktivitas tercatat secara akurat. Keamanan ditingkatkan melalui kode verifikasi yang dikirimkan kepada pengguna saat login pertama kali dari perangkat baru. Hasil kuesioner menunjukkan tingkat kepuasan pengguna yang tinggi, dengan skor rata-rata 85%, menunjukkan peningkatan dalam kenyamanan login, pengelolaan akun, dan pemantauan sistem. Implementasi ini terbukti efektif dalam meningkatkan efisiensi akses dan memastikan otentikasi pengguna yang aman di seluruh aplikasi.

Cara mensitasi artikel:
V. Meidita, S. Arifin, D. Wahyuningsih, D.W. Widarti. ”Penerapan Teknologi Single Sign On (SSO)dengan Metode JSON Web Token untuk Meningkatkan Kemudahan Akses Pengguna.” *Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi (JTI-TKI), vol. 17, no. 1, pp. 56-65, Maret 2026, https://doi.org/10.36382/jti-tki.v17i1.696*

PENDAHULUAN

Perkembangan teknologi digital telah mendorong penggunaan berbagai aplikasi daring dalam lingkungan kerja sehari-hari. Pada perusahaan software house seperti VINSCODE, pengguna dituntut untuk mengakses banyak sistem dengan kredensial yang berbeda-beda. Situasi ini menimbulkan permasalahan seperti lupa kata sandi, keharusan login berulang, serta meningkatnya risiko keamanan akibat penggunaan kata sandi yang lemah atau berulang.

Permasalahan autentikasi semacam ini telah banyak ditemukan dalam penelitian sebelumnya, yaitu banyak pengguna yang lupa akun dan kata sandi mereka karena mereka memiliki terlalu banyak akun untuk setiap sistem/aplikasi di lingkungan universitas, terdapat layanan aplikasi berbasis web, seperti Bagian Akademik, Sistem Informasi (SIA), dan E-Learning [1]. Solusi yang mulai banyak digunakan untuk mengatasi hal tersebut adalah teknologi Single Sign-On (SSO). SSO memungkinkan pengguna melakukan satu kali login untuk mengakses berbagai aplikasi terintegrasi tanpa harus mengulangi proses autentikasi. Dengan demikian, SSO dapat meningkatkan efisiensi akses sekaligus memperkuat kenyamanan pengguna.

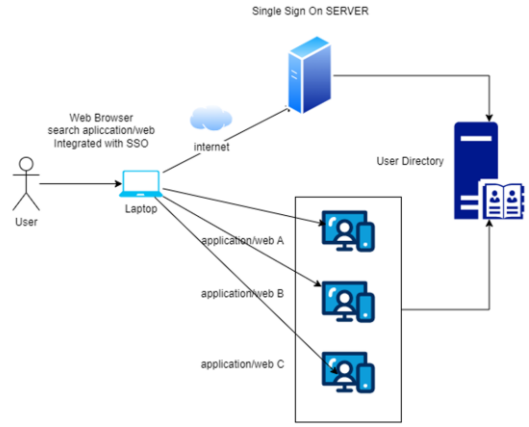
Dalam penelitian ini, teknologi SSO diterapkan menggunakan metode JSON Web Token (JWT) yang berfungsi sebagai token autentikasi. JWT memiliki kemampuan untuk membawa informasi pengguna secara aman dalam bentuk token digital, sehingga proses autentikasi menjadi lebih cepat dan ringan. Penggunaan JWT juga mendukung penerapan sistem pencatatan dan pelacakan aktivitas login pengguna secara terpusat [2][3].

Submitted 10 Juni 2026; Revised 19 Juni 2026; Accepted 19 Juni 2026

Tujuan dari penelitian ini adalah untuk mengimplementasikan teknologi SSO berbasis JWT pada perusahaan VINSCODE guna meningkatkan kemudahan akses pengguna, menyederhanakan proses login, serta menjaga keamanan data dan aktivitas login di berbagai aplikasi internal perusahaan.

Single Sign-On (SSO) merupakan teknologi yang memungkinkan pengguna melakukan satu kali proses autentikasi untuk mendapatkan akses ke berbagai aplikasi atau layanan yang saling terintegrasi. Teknologi ini bertujuan untuk mengurangi beban pengguna dalam mengingat banyak kredensial serta meningkatkan efisiensi dalam proses login. Dengan SSO, pengguna tidak perlu melakukan login ulang pada setiap layanan, karena sesi autentikasi telah dikelola secara terpusat oleh sistem. Hal ini memberikan keuntungan dalam hal kenyamanan dan keamanan akses terhadap sistem informasi [4].

JSON Web Token (JWT) adalah metode populer dalam sistem autentikasi modern, khususnya pada penerapan teknologi SSO. JWT digunakan untuk mengirimkan klaim identitas pengguna dalam bentuk token digital yang aman dan efisien. Token ini terdiri dari tiga bagian utama, yaitu header, payload, dan signature, yang dikodekan dalam format Base64 dan dapat diverifikasi oleh server tanpa menyimpan informasi sesi pengguna. JWT menjadi pilihan utama dalam implementasi SSO karena kemampuannya untuk menyimpan informasi identitas secara ringkas dan terenkripsi, serta dapat dikirimkan melalui HTTP header [5].



Gambar 1. Arsitektur Protokol Single Sign On (SSO)

Beberapa penelitian sebelumnya telah dilakukan untuk mengembangkan sistem autentikasi berbasis SSO. Salah satunya adalah penelitian yang mengkaji penerapan SSO menggunakan Cloud Identity di lingkungan kampus Politeknik Negeri Tanah Laut [6]. Penelitian tersebut menunjukkan bahwa SSO dapat mempermudah proses login pengguna, namun tidak secara spesifik mengukur aspek keamanan token maupun pelacakan aktivitas pengguna.

Penelitian ini berbeda dari penelitian sebelumnya karena menggunakan metode JWT sebagai dasar dalam penerapan SSO, serta melakukan pengujian terhadap tiga aspek utama, yaitu kemudahan akses pengguna, keamanan data, dan kemampuan pencatatan aktivitas login. Sistem yang dikembangkan tidak hanya memungkinkan pengguna mengakses beberapa website dengan satu kali login, tetapi juga mencatat riwayat perpindahan antar situs dan menerapkan kode verifikasi saat login dari perangkat baru. Dengan pendekatan ini, penelitian diharapkan dapat menunjukkan bahwa teknologi SSO berbasis JWT dapat meningkatkan efisiensi akses dan menjamin keamanan autentikasi pengguna dalam lingkungan aplikasi perusahaan [7].

Kebaruan dalam penelitian ini terletak pada pemilihan algoritma kriptografi RSA sebagai pengganti, menggantikan penggunaan HMAC yang lebih umum. Seperti yang dijelaskan pada algoritma kriptografi HMAC termasuk pada jenis algoritma kriptografi simetris yang dimana hanya menggunakan satu kunci pada proses enkripsi dan dekripsi nya. Sedangkan pada RSA yang termasuk pada algoritma kriptograsi asimetris yang memiliki kunci publik dan kunci pribada dalam proses enkripsi dan dekripsinya [8][9].

Dengan menerapkan algoritma RSA, penelitian ini mengeksplorasi pendekatan keamanan yang berbeda dalam pertukaran token otentikasi. RSA menawarkan keamanan yang tinggi melalui kunci publik dan pribadi, memastikan integritas dan keaslian token. Pendekatan ini diharapkan dapat memberikan lapisan keamanan tambahan dalam pengelolaan otentikasi pengguna dan pertukaran informasi dalam lingkungan SSO. Dengan demikian, kontribusi penelitian ini adalah memberikan alternatif keamanan yang cermat dan efektif dalam implementasi SSO dengan JWT, memperkuat aspek keamanan dalam pertukaran informasi otentikasi pengguna [10][11].

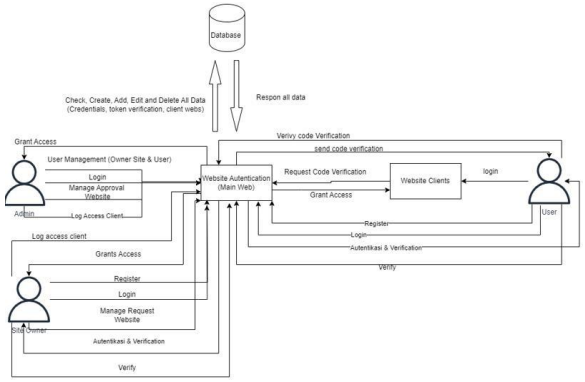
METODE

Metode Rancangan kegiatan dalam penelitian ini diawali dengan proses analisis kebutuhan terhadap sistem autentikasi tunggal untuk menghubungkan beberapa aplikasi internal dalam lingkungan kerja perusahaan VINSCODE. Solusi yang diimplementasikan adalah penerapan teknologi Single Sign-On (SSO) menggunakan metode JSON Web Token (JWT) sebagai sarana autentikasi dan otorisasi pengguna.

Sistem dirancang dengan tiga komponen utama, yaitu website authentication sebagai pusat autentikasi, website owner sebagai pemilik aplikasi, dan website client sebagai pengguna akhir. Hubungan antar komponen dijelaskan melalui sebuah diagram kerangka kerja sistem.

A. Gambaran Umum Kerangka Kerja (Framework)

Kerangka kerja dari sistem Single Sign On (SSO) berupa diagram UML dengan 3 aktor berbeda dijabarkan pada gambar 2 berikut.



Gambar 2. Framework Sistem Single Sign-On Berbasis JWT

Tahapan-tahapan pada aktor "Admin" sebagai berikut:

- Admin melakukan login dengan menggunakan kredensialnya seperti username/email dan password untuk masuk (login) ke website authentication.
- Admin dapat mengelola berbagai parameter pada web (User Management), termasuk menambah, mengedit, atau menghapus dan pengaturan CRUD
- Admin dapat melakukan approval website yang nantinya sebagai menyetujui website atau menolak website yang telah direquest oleh site owner.
- Admin juga dapat melihat riwayat akses log client

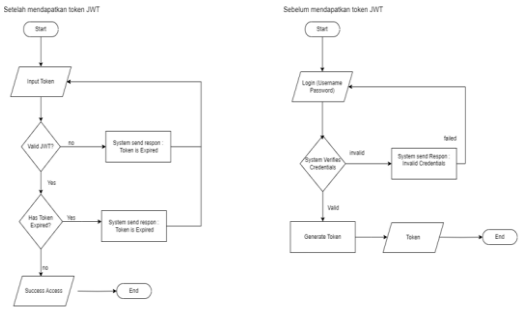
Tahapan-tahapan pada aktor "Site Owner" sebagai berikut:

- Site Owner melakukan pendaftaran (Register) di website authentication di sistem.
- Site Owner menggunakan kredensialnya seperti username/email dan password untuk masuk (login) ke website authentication.
- Setelah masuk, admin melakukan proses autentikasi dengan menggunakan kode (JSON Web Token dengan Kriptogtafi RSA) yang diberikan oleh sistem.
- Site Owner juga dapat mengelola berbagai parameter pada web (Website Management), termasuk menambah, mengedit, atau menghapus fitur dan pengaturan (CRUD).
- Site Owner juga dapat melihat riwayat akses log client

Tahapan-tahapan input-process-output pada aktor "User" sebagai berikut:

- Pengguna melakukan register pada website authentication untuk membuat akun.
- Setelah register, pengguna masuk ke website authentication menggunakan informasi kredensialnya (login).
- Pengguna melakukan proses autentikasi pada web website authentication menggunakan mekanisme yang melibatkan kode unik atau token (JSON Web Token dan Algoritma Kriptografi RSA).
- Setelah berhasil, pengguna masuk ke web/app client yang diinginkan.
- Di web/app client, pengguna memicu permintaan autentikasi yang dikirimkan ke sistem utama.
- Sistem utama memeriksa keberadaan data yang diminta, jika ditemukan maka sistem memberikan izin akses (Grant Access) ke web/app client.

B. Flowchart JSON Web Token



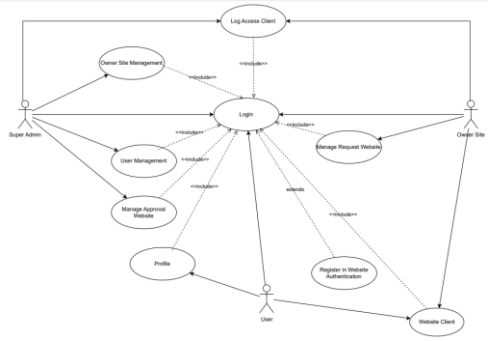
Gambar 3. Flowchart JSON Web Token (JWT)

Proses autentikasi dalam sistem dimulai dari pengguna yang melakukan login ke website authentication. Sistem kemudian memverifikasi data, dan jika valid, sistem akan menerbitkan token dalam bentuk JSON Web Token (JWT). Flowchart yang digunakan menggambarkan secara rinci proses sebelum dan sesudah pengguna mendapatkan token, termasuk bagaimana token tersebut digunakan untuk mengakses aplikasi lain tanpa perlu login ulang.

Setelah token diterbitkan, pengguna dapat mengakses berbagai aplikasi yang terintegrasi dalam sistem SSO.

C. Use Case Diagram & Activity Diagram

Untuk menggambarkan peran dan interaksi antara pengguna dan sistem secara menyeluruh, digunakan pendekatan use case diagram. Diagram ini memetakan aktor utama seperti admin, site owner, dan user, serta fungsi-fungsi yang tersedia bagi masing-masing.



Gambar 4. Use Case Diagram Sistem SSO

Selain itu, untuk menggambarkan alur kerja sistem secara lebih rinci, digunakan sejumlah activity diagram yang menunjukkan proses-proses utama dalam sistem. Diagram ini menggambarkan tahapan interaksi pengguna dengan sistem, mulai dari login awal oleh admin, registrasi pengguna baru, hingga proses verifikasi token saat menggunakan fitur SSO.

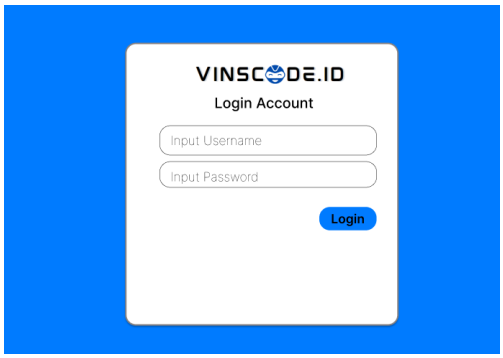
D. Rancangan Desain Antarmuka (Interface)

Perancangan antarmuka pengguna pada sistem ini bertujuan untuk mendukung kemudahan akses dan pemisahan peran berdasarkan fungsinya dalam proses autentikasi Single Sign-On (SSO). Antarmuka dirancang menggunakan aplikasi Figma dengan pendekatan berbasis peran, mencakup admin, site owner, user, dan client.

Setiap peran memiliki halaman antarmuka yang berbeda sesuai dengan tugas dan hak akses masing-masing. Website authentication menyediakan halaman login utama yang digunakan oleh semua pengguna untuk melakukan autentikasi pertama kali. Setelah berhasil login, pengguna diarahkan ke layanan masing-masing sesuai perannya. Site owner memiliki halaman pengelolaan aplikasi, sementara pengguna akhir akan menerima verifikasi token sebelum mengakses layanan klien.

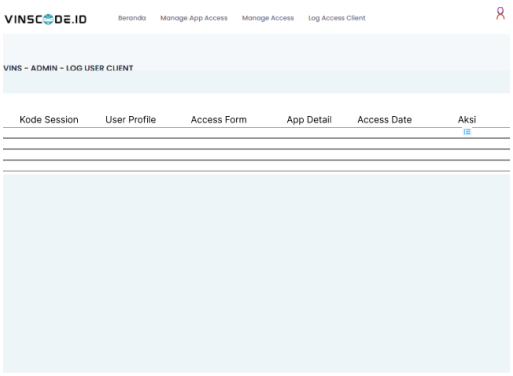
Ditampilkan interface tampilan halaman login utama sebagai pusat authentication, dan tampilan interface halaman log access client yang fungsinya sebagai pelacakan session yang nantinya site owner bisa melakukan pengecekan website mana saja yang diakses oleh user. Lalu ditampilkan juga halaman verifikasi akses pengguna sebagai bagian penting dari proses SSO

Selain itu, untuk menggambarkan alur kerja sistem secara lebih rinci, digunakan sejumlah activity diagram yang menunjukkan proses-proses utama dalam sistem. Diagram ini menggambarkan tahapan interaksi pengguna dengan sistem, mulai dari login awal oleh admin, registrasi pengguna baru, hingga proses verifikasi token saat menggunakan fitur SSO.



Gambar 5. Interface Halaman Login Website Authentication

Pada gambar 5 hanya admin yang dapat masuk ke website authentication dengan cara memasukkan username dan password yang benar.



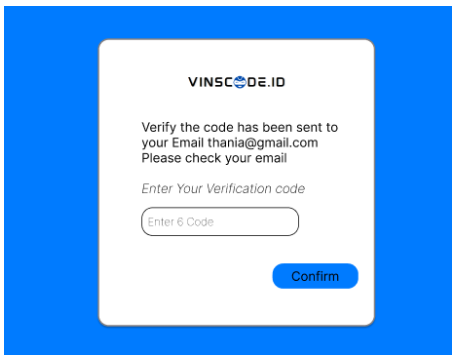
Gambar 6. Interface Halaman Log Access Client

Pada gambar 6 menampilkan halaman log session, yang dimana admin utama dan owner site bisa melakukan pelacakan user atau karyawan login di website yang terintegrasi dengan SSO.

Melakukan uji coba untuk mengakses website yang sudah terintergrasi dengan SSO, dengan login menggunakan SSO. Caranya masukkan terlebih dahulu username dan password user(pengguna).

Gambar 7. Interface Halaman Verifikasi Login SSO

Pada gambar 7 menunjukkan halaman verifikasi sesuai akun dan menampilkan akun yang sudah terintegrasi dengan SSO.



Gambar 8. Interface Halaman Input Kode Token

Pada gambar 8 menampilkan halaman verifikasi kode yang terkirim pada pemilik akun tersebut. Pada tahap tersebut permintaan kode akan terkirim ke akun pemilik. Setelah pada tahap verifikasi yang dimasukkan kode yang tepat, maka berhasil untuk masuk ke website tujuan.

E. Alat Pengujian

Untuk mendukung proses implementasi dan pengujian sistem, digunakan sejumlah alat bantu berupa perangkat keras dan lunak yang sesuai dengan kebutuhan pengembangan web. Perangkat yang digunakan meliputi laptop dengan spesifikasi standar pengembangan sistem serta perangkat lunak pendukung seperti web server, editor kode, dan framework pemrograman.

Tabel 1. Daftar Alat Pengujian Sistem (Hardware)

Nama Hardaware	Spesifikasi
Laptop Merk MSI Tipe GL63	• Processor Intel Core i7 Generasi 8 • RAM 8 GB • SSD 256 GB • VGA NVIDIA GEFORCE GTX • Koneksi Internet Provider MNC • Web Server Nginx • Backup Storage
Komputer	• Processor Ryzen 9 Generasi 7 • RAM 32 GB • SSD 256 GB • Web Server Nginx

Tabel 2. Daftar Alat Pengujian Sistem (Software)

Nama Software	Fungsi
Figma	Aplikasi yang digunakan untuk membuat desain prototipe UI/UX
Draw.io	Aplikasi diagram dan visualisasi yang memungkinkan pengguna membuat berbagai jenis diagram, termasuk diagram alur, diagram organisasi, diagram jaringan, dan banyak lagi.
Visual Studio Code	Sebuah aplikasi editor teks sumber terbuka (Open Source)
MySQL	Digunakan untuk server dan penyimpanan database.
Bahasa Pemrogaman PHP	Digunakan untuk menjalankan query SQL di database MySQL.

F. Parameter Pengujian

Pengujian dilakukan untuk membandingkan efektivitas sistem autentikasi yang sebelumnya digunakan di perusahaan dengan sistem baru berbasis Single Sign-On (SSO) menggunakan JSON Web Token (JWT). Pengujian ini bertujuan untuk menilai sejauh mana sistem baru dapat meningkatkan kemudahan akses, efisiensi login, pencatatan aktivitas, dan keamanan pengguna.

Sistem sebelumnya mengharuskan pengguna untuk login secara manual ke setiap aplikasi dengan kredensial yang berbeda-beda, yang menimbulkan kendala dalam hal pengalaman pengguna dan keamanan. Sistem usulan mengintegrasikan proses login hanya satu kali di awal, dan selanjutnya pengguna dapat berpindah antar aplikasi tanpa harus melakukan login ulang.

Tabel 3. Parameter Perbandingan Sistem Autentikasi

No	Pengujian	Kemudahan Akses	Pencatatan/ Pelacakan	Keamanan Data
1	Login ke Website Pertama			
2	Login ke Website Pertama, pindah ke website kedua			
3	Login ke Website Pertama, pindah ke Website Kedua, lalu pindah ke Website Ketiga			
4	Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, lalu pindah ke Website keempat			
5	Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, pindah ke Website keempat. Lalu terakhir pindah ke Website kelima			

Perbandingan ini dilakukan berdasarkan tiga indikator utama: kemudahan akses pengguna, pencatatan dan pelacakan aktivitas login, serta keamanan data. Dengan mengacu pada indikator tersebut, sistem baru diharapkan mampu memberikan pengalaman login yang lebih efisien dan aman

G. Rancangan Pengujian Kuesioner

Pengujian sistem juga dilakukan melalui penyebaran kuesioner kepada pengguna untuk memperoleh penilaian subjektif terhadap sistem yang telah diimplementasikan. Kuesioner disusun untuk mengukur tingkat kepuasan pengguna berdasarkan tiga indikator utama yang telah ditentukan sebelumnya, yaitu kemudahan akses pengguna, pencatatan dan pelacakan aktivitas login, serta keamanan data.

Instrumen kuesioner ini disusun dengan mengadopsi metode dari penelitian Fathurrahmani, Herpendi, dan Khairul (2021), dengan penyesuaian terhadap konteks penerapan sistem SSO berbasis JSON Web Token (JWT) di perusahaan VINSCODE. Setiap pernyataan dinilai menggunakan skala Likert 5 poin, mulai dari “sangat tidak setuju” hingga “sangat setuju”

Tabel 4. Pernyataan Kuesioner Pengujian Sistem SSO

No	Pertanyaan	Jawaban				
		SS	S	CS	KS	TS
1	Pengguna terbebani dengan mengingat Username dan Password untuk beberapa website					
2	Dengan adanya SSO pengguna terbantukan dengan tidak perlunya mengingat banyak Username dan Password					
3	Penerapan SSO memudahkan pengguna untuk login ke website yang ada					
4	Kode verifikasi terkirim ke pengguna melalui email pengguna					
5	Monitoring session memudahkan untuk melihat akses login setiap akun					

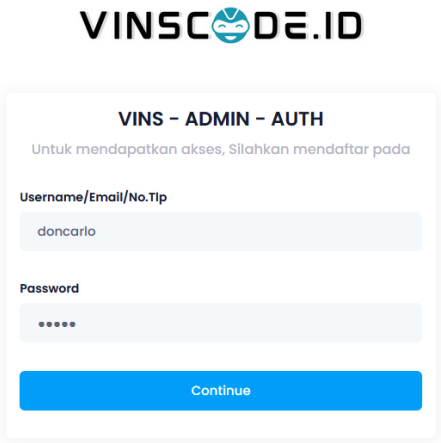
Kuesioner ini disebarkan kepada responden dari internal perusahaan yang telah mencoba langsung penggunaan sistem. Hasil dari kuisioner ini menjadi dasar untuk menilai kepuasan pengguna terhadap sistem yang dikembangkan, serta untuk menguatkan hasil dari uji fungsional dan teknis yang telah dilakukan sebelumnya.

HASIL DAN PEMBAHASAN

A. Hasil Pengujian Sistem

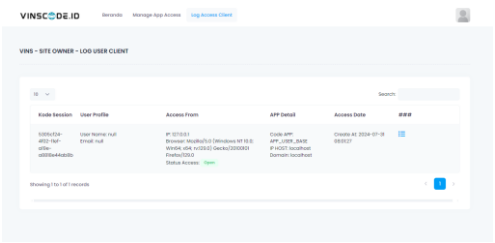
Hasil implementasi sistem menunjukkan bahwa penerapan Single Sign-On (SSO) berbasis JSON Web Token (JWT) berhasil meningkatkan kemudahan akses pengguna. Sebelumnya, pengguna harus login secara terpisah ke setiap aplikasi yang digunakan. Setelah sistem SSO diterapkan, pengguna cukup melakukan satu kali login melalui website authentication untuk dapat mengakses seluruh aplikasi yang terintegrasi, seperti website client dan website owner.

Pengujian dilakukan dengan melakukan login menggunakan satu akun ke dalam portal utama, kemudian pengguna diarahkan langsung ke layanan lain tanpa diminta login ulang. Proses ini dapat berjalan secara otomatis karena token autentikasi yang dikirimkan disimpan dalam browser dan digunakan kembali saat pengguna mengakses aplikasi lain yang terhubung. Beriut akan ditampilkan hasil dari login authentication, hasil tampilan halaman fitur untul log access client yaitu sebagai fitur pelacakan dan pencatatn perpindahan antara website, lalu hasil tampilan alur proses verifikasi akses pengguna sebagai bagian penting dari proses SSO.



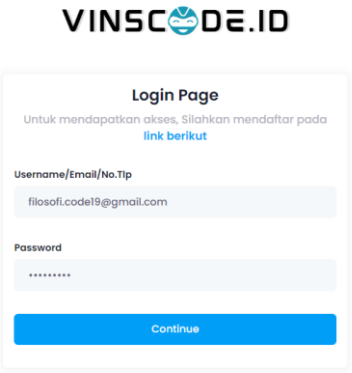
Gambar 9. Halaman Login Website Authentication

Pada gambar 9 menampilkan halaman login pada Website Autentikasi, yaitu sebagi pusat authentication termasuk website client yang terintegrasi dengan SSO.

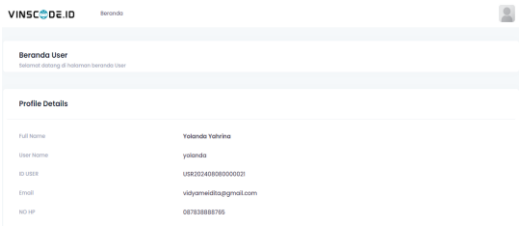


Gambar 10. Halaman Log Aktivitas Pengguna

Halaman khusus disediakan untuk admin dalam memantau aktivitas pengguna, di mana setiap login tercatat secara otomatis. Admin dapat mengetahui aktivitas pengguna, seperti perpindahan antar situs dan sesi login yang belum ditutup. Hal ini mendukung aspek keamanan dan audit sistem secara menyeluruh.



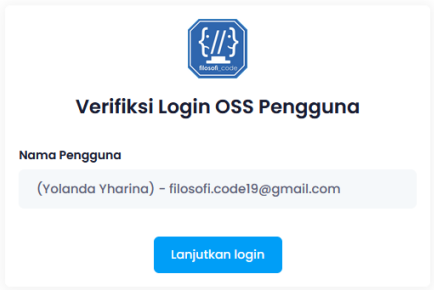
Gambar 11. Tampilan Halaman Login Pertama ke Website User



Gambar 12. Tampilan Halaman Profile User

Dengan adanya fitur Log Access Client pada gambar 10, proses monitoring menjadi lebih mudah dan efisien, serta mendukung transparansi dalam penggunaan sistem oleh setiap peran pengguna di perusahaan. Fitur pencatatan aktivitas pengguna menjadi salah satu keunggulan dalam sistem SSO yang diimplementasikan. Sistem ini memungkinkan admin untuk melihat riwayat login pengguna secara real-time, termasuk informasi waktu akses, situs yang diakses, dan sesi login yang sedang aktif.

Pada gambar 12 menampilkan halaman user yang tandanya sudah berhasil memasuki profile dengan menggunakan akun tersebut. Setelah sudah berhasil login. User dapat mencoba login menggunakan SSO untuk login ke beberapa website. User juga bisa langsung melakan cara lain seperti langsung login dengan SSO ke website client maka otomatis user juga sudah login ke halaman profile dan otomasi login juga di beberapa website yang terintegrasi dengan SSO



Gambar 13. Halaman Verifikasi Login dengan SSO

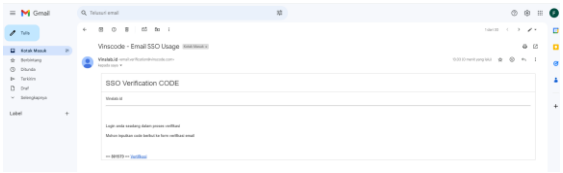
Pada gambar 13 otomatis akan ditampilkan nama akun pengguna yang sudah terverifikasi di sistem SSO. Karena user sebelumnya sudah login terlebih dahulu ke halaman profile. Setelah sudah melakukan beberapa tahap verifikasi seperti input kode verifikasi maka user bisa langsung akses beberapa halaman website tanpa login ulang.

Pada gambar 13 hingga gambar 15 menampilkan proses login pertama pengguna ke website user, lalu setelah sudah melakukan login pertama tidak perlu melakukan login kembali untuk masuk beberapa website. Dengan begitu akan mempersingkat waktu autentikasi dan memberikan pengalaman penggunaan yang lebih efisien, khususnya bagi pengguna yang harus berpindah antar aplikasi secara berkala dalam pekerjaan sehari-hari. Dengan adanya sistem ini, pengguna tidak perlu lagi mengingat banyak kredensial maupun mengulang proses login untuk setiap aplikasi.

Untuk menjaga keamanan akses pengguna, sistem dilengkapi dengan mekanisme verifikasi tambahan saat login dari perangkat yang belum dikenali sebelumnya. Setelah memasukkan kredensial login, pengguna akan diminta memasukkan kode verifikasi yang dikirimkan melalui email. Hal ini bertujuan untuk memastikan bahwa hanya pengguna yang sah yang dapat melanjutkan proses login. Fitur ini diuji dengan melakukan login dari browser atau perangkat berbeda, dan sistem secara otomatis menampilkan halaman verifikasi token. Pengguna harus memasukkan kode verifikasi terlebih dahulu sebelum dapat mengakses aplikasi yang diinginkan.

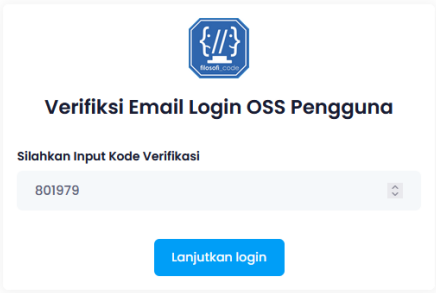
Gambar 14. Halaman Verifikasi Email Login SSO

Pada gambar 14 sistem mengirimkan kode token ke email pengguna. Kemudian pengguna dapat mengisikan kode verifikasi yang telah terkirimkan melalui email.



Gambar 15. Email Pengguna

Pengguna bisa melakukan pengecekan kode verifikasi yang dikirimkan dari sistem dan dikirim melalui email pengguna. Gambar 18 menjelaskan mengenai proses, apabila user sudah memasukan kode verifikasi sesuai dengan benar, maka user bisa langsung masuk ke beberapa website clinet tanpa login ulang.



Gambar 16. Input Kode Verifikasi dari Email

B. Hasil Parameter Pengujian

Tabel 5. Hasil Parameter Pengujian Metode Lama

Pengujian	Kemudahan Akses	Pecatatan & Pelacakan	Keamanan Data
Login ke Website Pertama	Login tanpa sso dan login pertama kali dengan username dan password.	Tidak ada pencatatan dan pelacakan login atau sesi pengguna	Tidak ada verifikasi dan autentikasi akun pengguna
Login ke Website Pertama, pindah ke website kedua	Melakukan login ulang di website kedua	Tidak ada pencatatan dan pelacakan login atau sesi pengguna	Tidak ada verifikasi dan autenti kasi akun penggu na
Login ke Website Pertama, pindah ke Website Kedua, lalu pindah ke Website Ketiga	Melakukan login ulang di website ketiga	Tidak ada pencatatan dan pelacakan login atau sesi pengguna	Tidak ada verifikasi dan autentikasi akun pengguna
Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, lalu pindah ke website keempat	Melakukan login ulang di website keempat	Tidak ada pencatatan dan pelacakan login atau sesi pengguna	Tidak ada verifikasi dan autentikasi akun pengguna
Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, pindah ke website keempat. Lalu terakhir pindah ke website kelima	Melakukan login ulang di website kelima	Tidak ada pencatatan dan pelacakan login atau sesi pengguna	Tidak ada verifikasi dan autentikasi akun pengguna

Parameter Pengujian dilakukan untuk membandingkan efektivitas sistem autentikasi yang lama dengan sistem baru berbasis Single Sign-On (SSO) menggunakan JSON Web Token (JWT). Tiga parameter utama yang digunakan sebagai dasar pengujian adalah: kemudahan akses pengguna, pencatatan dan pelacakan aktivitas login, serta keamanan data.

Pada metode lama, pengguna harus login ke setiap website secara terpisah dengan akun berbeda, yang menyebabkan pengalaman penggunaan menjadi tidak efisien dan berpotensi mengurangi keamanan karena penggunaan kata sandi yang sama. Sistem juga tidak mencatat aktivitas login pengguna secara terpusat, sehingga sulit untuk melakukan pelacakan.

Tabel 6. Hasil Parameter Pengujian Metode Yang Diusulkan (Baru)

Pengujian	Kemudahan Akses	Pecatatan & Pelacakan	Keamanan Data
Login ke Website Pertama	Login dengan sso di website pertama	Tercatat aktivitas login di website pertama	Sistem mengirim kode verifikasi ke akun pengguna saat pertama kali login di website pertama
Login ke Website Pertama, pindah ke website kedua	Tidak perlu login ulang di website kedua	Tercatat aktivitas perpinda h login dari website pertama ke website kedua	Pengguna bisa langsung masuk ke halaman website kedua tanpa verifikasi ulang
Login ke Website Pertama, pindah ke Website Kedua, lalu pindah ke Website Ketiga	Tidak perlu login ulang di website ketiga.	Tercatat aktivitas perpinda h login dari website pertama hingga website ketiga	Pengguna bisa langsung masuk ke halaman website ketiga tanpa verifikasi ulang
Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, lalu pindah ke website keempat	Tidak perlu login ulang di website keempat	Tercatat aktivitas perpindah login dari website pertama hingga ke website keempat	Pengguna bisa langsung masuk ke halaman website keempat tanpa verifikasi ulang
Login ke Website Pertama, pindah ke Website Kedua, pindah ke Website Ketiga, pindah ke website keempat. Lalu terakhir pindah ke website kelima	Tidak perlu login ulang di website kelima.	Tercatat aktivitas perpinda h login dari website pertama ke website kelima	Pengguna bisa langsung masuk ke halaman website kedua tanpa verifikasi ulang

Sebaliknya, sistem usulan memungkinkan pengguna melakukan satu kali login untuk mengakses semua layanan yang terintegrasi. Token JWT digunakan untuk mendistribusikan autentikasi, dan aktivitas pengguna

dapat dipantau melalui sistem logging yang terpusat. Selain itu, sistem juga menyediakan mekanisme verifikasi tambahan saat login dari perangkat baru untuk meningkatkan keamanan. Berikut hasil parameter pengujian metode lama dan hasil parameter pengujian d dari metode yang di usulkan (Metode SSO dengan JWT).

Dari hasil ini dapat disimpulkan bahwa sistem yang diusulkan memberikan peningkatan nyata dalam kemudahan akses, keamanan data, serta kemampuan pelacakan aktivitas pengguna dibandingkan sistem autentikasi sebelumnya.

C. Hasil Kuesioner Pengujian

Untuk mendukung pengujian sistem secara subjektif, dilakukan penyebaran kuesioner kepada 30 orang responden yang telah menggunakan sistem Single Sign- On (SSO) berbasis JSON Web Token (JWT). Kuesioner disusun berdasarkan skala Likert dengan lima tingkatpenilaian, mulai dari "Sangat Tidak Setuju" hingga "Sangat Setuju", dan mengacu pada indikator kemudahan akses, keamanan data, serta pelacakan aktivitas pengguna.

Setiap pertanyaan dirancang untuk menilai pengalaman pengguna selama menggunakan sistem, termasuk beban mengingat akun, efisiensi login, keberhasilan verifikasi keamanan, dan kejelasan monitoring aktivitas. Hasil perolehan skor dikonversikan dalam bentuk persentase dan diinterpretasikan menurut rentang kategori nilai tingkat kepuasan.

Tabel 7. Hasil Rekapitulasi Hasil Pengujian Kuesioner SSO

No	Pernyataan	Skor (%)	Interpretasi
1	Pengguna terbebani mengingat banyak akun	81%	Sangat Setuju
2	SSO membantu mengurangi beban mengingat akun	86%	Sangat Setuju
3	SSO memudahkan login ke berbagai website	90%	Sangat Setuju
4	Kode verifikasi terkirim ke email saat login dari perangkat baru	91%	Sangat Setuju
5	Monitoring session memudahkan melihat akses login pengguna	78%	Setuju
Rata-rata		85%	Sangat Setuju

Berdasarkan hasil tersebut, dapat disimpulkan bahwa sebagian besar pengguna merasa puas terhadap sistem SSO yang telah dikembangkan. Nilai rata-rata keseluruhan sebesar 85% mengindikasikan bahwa sistem berhasil memenuhi ekspektasi dari sisi kemudahan penggunaan, keamanan, dan manajemen autentikasi pengguna.

KESIMPULAN DAN SARAN

Penerapan teknologi Single Sign-On (SSO) berbasis JSON Web Token (JWT) di perusahaan VINSCODE berhasil meningkatkan kemudahan akses pengguna, pencatatan aktivitas login, dan keamanan data. Sistem memungkinkan login tunggal untuk berbagai aplikasi, mencatat aktivitas secara terpusat, serta menambahkan verifikasi keamanan saat login dari perangkat baru. Hasil kuisioner menunjukkan tingkat kepuasan pengguna sebesar 85% yang termasuk kategori "sangat setuju". Ke depan, sistem ini dapat dikembangkan lebih lanjut dengan peningkatan keamanan token serta dokumentasi teknis agar mudah diintegrasikan pada proyek lain.

UCAPAN TERIMA KASIH

Penulis menyampaikan penghargaan dan terima kasih kepada Bapak dan Ibu selaku dosen pembimbing atas arahan, dukungan, dan evaluasi yang konstruktif selama proses penyusunan artikel ini. Ucapan terima kasih juga disampaikan kepada pihak perusahaan VINSCODE yang telah memberikan izin, data, serta dukungan teknis dalam implementasi dan pengujian sistem. Kontribusi dari seluruh pihak terkait telah memberikan dampak signifikan terhadap kelancaran dan penyelesaian artikel ilmiah ini.

REFERENSI

[1] Waluyo, T., & Sutarman. (2022). Comparative Analysis of the Performance of Single . International Journal of Computer and Information Technology, 100-106.
[2] Syabdan, D., Joeharsyah, R., & Asep, M. (2022). THE MODEL FOR STORING TOKENS IN LOCAL STORAGE (COOKIES). Journal of Applied Engineering and Technological Science, 149-155.
[3] Murilo, G. d., & Edna, D. C. (2022). Authentication and Authorization in Microservices. https://www.mdpi.com/journal/applsci, 1-20.
[4] I.I., K., M.V., K., I.S., G., & P.V., K. (2021). Developing a single sign-on for information systems. Software Journal: Theory and Applications, 1-9.
[5] Rohmat, G., & Alam, R. (2019). JSON Web Token (JWT) untuk Authentication pada Interoperabilitas Arsitektur berbasis RESTful Web Service. Jurnal Edukasidan Penelitian Informatika, 74-79.
[6] Fathurrahmani, Herpendi, & Khairul, A. (2021). PERANCANGAN SINGLE SIGN ON(SSO)PADA APLIKASI WEB MENGGUNAKAN CLOUD IDENTITY (STUDI KASUS:POLITEKNIK NEGERI TANAH LAUT). Jurnal Ilmiah Teknik Informatika, 242-251.
[7] Rahmatulloh, Gunawan, & Nursuwars. (2019). Performance comparison of signed algorithms on JSON Web. IOP Conference Series: Materials Science and Engineering, 1-8.
[8] Albert, G., Rizal, I., & Ike, P. W. (2015). Implementasi Algoritma Kriptografi RSA Untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi dan Sistem Komputer , 253-258.
[9] Basri. (2016). KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI. Jurnal Ilmiah Ilmu Komputer, 16-23.
[10] Bonie, E. G. (2022). PENERAPAN KRIPTOGRAFI DENGAN METODE RSA PADA INTERNET BANKING (STUDI KASUS: SECURITY TOKEN DAN SMART CARD). Jurnal Teknologi Informasi, 1-7.
[11] Mustafa, T. (2020). Design and Implementation of Blockchain Based Single Sign-On. SAKARYA UNIVERSITY JOURNAL OF

COMPUTER AND INFORMATION SCIENCES, 343-354.