*Journal of Information Technology and Computer Science (INTECOMS)*
Volume 6 Nomor 2, Desember 2023
e-ISSN : 2614-1574
p-ISSN : 2621-3249

# MODEL IMPLEMENTASI NFT PADA WEB SSO MELALUI PROTOKOL OPENID CONNECT DAN OAUTH 2.0

## *MODEL OF NFT IMPLEMENTATION ON WEB SSO OVER OPENID CONNECT AND OAUTH 2.0 PROTOCOLS*

**Esa Fauzi[1], Sy Yuliani[2], Yenie Syukriyah[3], Azizah Zakiah[4]**
[1,2,3,4]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Widyatama, Bandung, Indonesia
esa.fauzi@widyatama.ac.id[1], sy.yuliani@widyatama.ac.id[2], yenie.syukriyah@widyatama.ac.id[3], azizah.zakiah@widyatama.ac.id[4]

***ABSTRACT***

*Single Sign-On (SSO) is a mechanism that allows users to access various services using a single set of login credentials. However, in SSO implementations, there are still challenges related to security and authentication management, particularly attacks targeting the Identity Provider (IDP). To address this, the use of Non-Fungible Tokens (NFTs) as proof of IDP ownership has been proposed as a solution to enhance security in the authentication mechanism. The utilization of NFTs in SSO with OpenID Connect and OAuth 2.0 has the potential to improve security and convenience in the authentication process due to the unique and non-duplicable nature of NFTs. The results of this research present a model and design of SSO with NFTs on OpenID Connect and OAuth 2.0. An SSO application with login, register, and password recovery features was also developed to provide convenience to users during the login process. The findings conclude that the utilization of NFTs in SSO with OpenID Connect and OAuth 2.0 has the potential to enhance security and convenience in the authentication mechanism. Further research is needed to explore aspects such as scalability, in-depth security analysis, testing in real-world scenarios, improvement of integration and interoperability, as well as comparative analysis with other SSO technologies.*

**Keywords:** *SSO, NFT, OpenID Connect, OAuth2*

**ABSTRAK**

Single Sign-On (SSO) adalah mekanisme yang memungkinkan pengguna untuk mengakses berbagai layanan dengan menggunakan satu set kredensial login. Namun, dalam implementasi SSO, masih ada tantangan terkait keamanan dan manajemen otentikasi, salah satunya serangan kepada Identiy Provider (IDP). Untuk mengatasi ini, penggunaan Non-Fungible Token (NFT) sebagai bukti kepemilikan Identity Provider (IDP) diusulkan sebagai solusi yang dapat meningkatkan keamanan dalam mekanisme otentikasi. Penggunaan NFT dalam SSO dengan OpenID Connect dan OAuth 2.0 memiliki potensi untuk meningkatkan keamanan dan kenyamanan dalam mekanisme otentikasi karena NFT bersifat unik atau tidak dapat di duplikasi. Hasil dari penelitian ini menghasilkan model dan rancangan SSO dengan NFT pada OpenIDConnect dan Oauth2. Aplikasi SSO dengan fitur login, register, dan lupa password juga dibangun untuk memberikan kemudahan pada pengguna ketika melakukan proses login. Dari hasil yang diperoleh disimpulkan bahwa penggunaan NFT dalam SSO dengan OpenID Connect dan OAuth 2.0 memiliki potensi untuk meningkatkan keamanan dan kenyamanan dalam mekanisme otentikasi. Penelitian selanjutnya perlu dilakukan untuk mengeksplorasi aspek-aspek seperti skalabilitas, analisis keamanan yang lebih mendalam, pengujian dalam skenario nyata, peningkatan integrasi dan interoperabilitas, serta analisis perbandingan dengan teknologi SSO lainnya.

**Kata Kunci:** SSO, NFT, OpenID Connect, OAuth2

## PENDAHULUAN

Jumlah pengguna internet di negara Indonesia pada Maret 2021 mencapai 212,35 juta dan menjadi peringkat ketiga dunia dibawah Tiongkok (Asnawi, 2022). Jumlah ini meningkat pesat dari sebelumnya 88,1 juta pada tahun 2014 (Iskandar & Isnaeni, 2019). Hal ini menunjukan masifnya perkembangan teknologi internet. Berkembangnya teknologi internet karena didukung dengan jumlah perkembangan aplikasi web juga yang semakin banyak.

Aplikasi web adalah aplikasi yang dijalankan di browser dan diakses melalui jaringan internet (Dissanayake & Diaz,

2017). Aplikasi web ini memiliki keunggulan karena tidak perlu di-*install* - dan dapat diakses dimana saja dibandingkan dengan aplikasi desktop. Karena keunggulan ini banyak perusahaan yang kemudian beralih dari aplikasi desktop ke aplikasi web. Namun karena dapat diakses melalui internet maka kebanyakan aplikasi memiliki proses otentifikasi dengan kredential seperti *username* dan *password* untuk menjaga data dari pihak yang berbahaya.

Terkadang dalam lingkungan bisnis pengguna sering kali harus memasukkan kredential mereka secara terpisah untuk mengakses berbagai aplikasi atau beberapa layanan yang mereka gunakan. Hal ini dapat menjadi rumit dan memakan waktu, terutama jika pengguna harus melakukan log in beberapa kali dalam sehari. SSO adalah salah satu teknologi untuk menangani masalah ini. SSO adalah teknologi yang memungkinkan user atau pengguna untuk menggunakan banyak layanan melalui otentifikasi *log in* satu akun saja (Nishioka & Okabe, 2020a).

Dalam pengembangannya banyak pendekatan atau metode yang bisa diterapkan dalam teknologi SSO, diantaranya adalah OAuth2.0 dan OpenID Connect. OAuth2.0 adalah framework atau protokol otorisasi sedangkan OpenID Connect adalah salah satu ekstensi yang bisa ditambahkan diatas OAuth2.0. OpenID Connect adalah salah satu ekstensi yang menambahkan lapisan otentifikasi menggunakan suatu identitas dan bersama OAuth 2.0, keduanya berinteraksi diantara *role-role* yang terdefinisi pada protokol OAuth 2.0 (Dodanduwa & Kaluthanthri, 2018). Dalam penelitian SSO ini, OpenID Connect dan OAuth2.0 digunakan karena memiliki kelebihan fleksibilitas dan kemudahan penggunaannya dalam menyediakan solusi untuk SSO(Ahammad Karim & Muhammad Abdullah Adnan, 2019). Namun dengan kelebihan ini, masih ada kekurangan yang bisa diperoleh dari penggunaan OpenID connect, salah satunya adalah dari sisi keamanan.

Dalam dua penelitian yang ditulis oleh Christian Mainka terdapat kerentanan serangan terhadap SSO yang menggunakan OpenID Connect. Penelitian pertama (Mladenov et al., 2016) membahas tentang ancaman keamanan pada sistem Single Sign-on (SSO) yang menyoroti kelemahan pada Identitas Provider (IdP) yang dapat membuka celah keamanan pada sistem SSO. Ancaman pada SSO ini dibagi menjadi 2 teknik serangan: ID Spoofing dan Key Confusion. "ID Spoofing" adalah teknik serangan di mana penyerang membuat IdP palsu untuk menipu pengguna untuk memasukkan informasi autentikasi mereka. Sedangkan "Key Confusion" merujuk pada serangan di mana penyerang mencoba untuk memperoleh kunci rahasia yang digunakan oleh IdP dalam proses autentikasi pengguna.

Penelitian kedua membahas tentang ancaman yang bisa terjadi pada OpenID connect. Terdapat 2 serangan yang dibahas, yaitu IdP Confusion dan Malicious Endpoint(Mainka et al., 2017). Serangan IdP confusion adalah serangan di mana penyerang memanipulasi metadata SSO untuk menipu pengguna agar memercayai identitas penyerang sebagai IdP yang sah. Dalam konteks OpenID Connect, metadata SSO adalah informasi yang digunakan oleh penyedia layanan untuk menemukan dan berinteraksi dengan server OpenID Connect. Dalam serangan ini, penyerang dapat memanipulasi metadata SSO sehingga pengguna diarahkan ke server OpenID Connect palsu yang dikendalikan oleh penyerang. Sedangkan serangan Malicious Endpoint adalah serangan di mana penyerang memanipulasi endpoint yang digunakan oleh penyedia layanan untuk berkomunikasi dengan server OpenID Connect. Dalam serangan ini, penyerang dapat mengirimkan endpoint palsu yang mengarahkan pengguna ke server OpenID Connect palsu yang dikendalikan oleh penyerang.

Berdasarkan pengamatan kami masih terdapat potensi ancaman keamanan dari penggunaan OpenID Connect dalam

penerapan SSO. Oleh karena itu kami mengajukan satu teknologi lagi dalam penerapan SSO untuk meningkatkan faktor keamanan yaitu teknologi blockchain NFT. NFT adalah unit data yang disimpan di buku besar digital blockchain untuk merepresentasikan item seperti foto, video, audio, dan kekayaan intelektual lainnya (Takahashi & Lakhani, 2021). NFT ini menyatakan aset digital sebagai unik yang tidak dapat dipertukarkan. Pada penelitian ini NFT digunakan sebagai bukti kepemilikan dikarenakan banyak serangan yang fokus mengekploitasi IdP pada OpenID Connect. NFT digunakan sebagai bukti kepemilikan untuk memverifikasi identitas pengguna.

Pada penelitian ini kami juga melakukan analisis terhadap beberapa penelitian terkait untuk memberikan gambaran dari teknologi yang bisa digunakan pada SSO. Lang Zhang dalam jurnal "*A New Identity Authentication Scheme of Single Sign On for Multi-Database*" mengusulkan sebuah skema otentikasi baru untuk akses single sign-on ke beberapa database (Zhang et al., 2016). Skema yang diusulkan memanfaatkan informasi identitas pengguna dan fungsi hash untuk menghasilkan kunci sesi, yang digunakan untuk otentikasi dan pengendalian akses. Skema juga mencakup mekanisme untuk mencegah serangan replay dan meningkatkan keamanan kata sandi. Jurnal ini kemudian menyimpulkan bahwa skema yang diusulkan menawarkan keamanan dan efisiensi yang lebih baik dibandingkan dengan skema otentikasi yang sudah ada.

Lalu terdapat juga penelitian oleh Spoorthi V dalam jurnalnya "*Mobile SSO Solution for Enterprise Cloud Aplication"* menggunakan PKI (*public Key Infrastucture)* sebagai kerangka kerja mengelola kunci publik, sertifikat digital, dan layanan keamanan lainnya yang berhubungan dengan kriptografi kunci public(Spoorthi & Sekaran, 2014). PKI digunakan untuk mengenkripsi dan menandatangani data yang dikirimkan antara pengguna dan aplikasi awan perusahaan. Sertifikat digital yang dikeluarkan oleh otoritas sertifikat (CA) digunakan untuk mengautentikasi identitas pengguna dan aplikasi yang terlibat dalam transaksi. Dengan menggunakan PKI, solusi SSO dapat memberikan lapisan keamanan tambahan untuk melindungi data pengguna dan mencegah akses yang tidak sah ke aplikasi *Enterprise Cloud.*

Selain itu, Teknologi SSO juga bisa digunakan di beberapa perangkat teknologi lain seperti Bluetooth, biometric, lightweight device, RFID, dan NFC. Dalam perangkat Bluetooth terdapat penelitian oleh Karishma Jain dalam jurnal "Single Sign On using Bluetooth device" (Jain & Shete, 2016). Jurnal ini membahas tentang penggunaan perangkat Bluetooth sebagai alat autentikasi dalam sistem Single Sign-On (SSO). Tujuan dari penelitian ini adalah untuk meningkatkan keamanan dan kenyamanan penggunaan SSO dengan menggunakan perangkat Bluetooth sebagai alat autentikasi tanpa memerlukan input manual seperti password atau PIN. Penerapannya memanfaatkan IBM Security Access Manager Enterprise Single SignOn (ISAMESSO) yang diintegrasikan dengan teknologi Bluetooth.

Penelitian lain dalam perangkat teknologi adalah pada biometrik yang ditulis oleh Di Liu dan Wenzheng Liu. Di Liu mengusulkan skema otentikasi pengguna Single Sign On berbasis biometrik baru dalam sistem Telematika, untuk memungkinkan melindungi privasi akun pengguna dan menggabungkan biometrik dengan Single Sign On untuk menggantikan cara otentikasi pengguna tradisional dengan kata sandi dalam sistem Telematika (D. Liu et al., 2012). Sedangkan penelitian oleh Di Liu mengginakan skema "ID-MAKA" (Identity-based Mutual Authenticated Key Agreement) yang terenkripsi untuk memastikan keamanan data dan privasi pengguna dimana terdapat registrasi biometrik untuk menghasilkan kunci publik dan kunci privat yang unik(W. Liu et al., 2019). Hal ini memastikan bahwa

tidak ada pihak ketiga yang dapat mengakses informasi pribadi pengguna

Selain itu terdapat juga penelitan SSO pada perangkat ligtweight device oleh Payal Sharma. Jurnal "*Hybrid Single Sign-On Protocol for Lightweight Devices*" membahas tentang protokol single sign-on (SSO) yang dikembangkan untuk perangkat ringan seperti ponsel pintar dan tablet. Protokol ini menggunakan metode otentikasi ganda (multi-factor authentication) dan teknologi kriptografi untuk memastikan keamanan data saat login (Sharma & Sihag, 2016). Dalam jurnal ini, dituliskan bahwa protokol SSO hibrida ini dapat digunakan secara efektif pada perangkat dengan sumber daya terbatas. Hasil eksperimen menunjukkan bahwa protokol yang diusulkan memiliki kinerja yang baik dan dapat menjadi alternatif yang lebih baik daripada protokol SSO yang ada pada perangkat yang lebih ringan.

Teknologi RFID (Radio Frequency Identification) dan NFC (Near Field Communication) yang merupakan teknologi komunikasi jarak pendek untuk pertukaran data dapat juga diterapkan pada SSO. Penelitian dengan RFID dilakukan oleh Zhuosheng Su di dalam lingkungan mobile menggunakan dinamik teken dan WMMP (Wireless M2M Protokol) untuk mengimplementasikan keamanan dan ototentifikasi dari Mobile RFID middleware (Su et al., 2013). Sedangkan penelitian dari Ufuk Cellikan menambahkan teknologi NFC sebagai keamanan tambahan dari SSO(*NFC Based Mobile Single Sign-on Solution as a Chrome Extension | IEEE Conference Publication | IEEE Xplore*, n.d.). NFC diintegrasikan dengan browser ekstensi menggunakan Java Applet. Ekstensi tersebut kemudian menyediakan akses untuk NFC reader dan sebagai jembatan antara Java dan Javascript di dalam browser. Dengan adanya NFC ini pengguna juga diberikan kemudahan dalam login dengan tanpa menginputkan username dan password-nya.

Selain OpenID Connect terdapat banyak juga metode yang bisa digunakan dalam pengembangan SSO seperti AJAX, Load Distribution Method, two-factor authentication, dan SAML. Penelitian SSO dengan AJAX dari Yang Te-Jun menawarkan SSO yang berbeda dari teknik SSO tradisional, yaitu ketika pengguna submit permintaan login, semua identitas otentifikasi dibawa secara konkuren; artinya, permintaan otentifikasi dikirim ke semua sub sistem pada waktu yang sama menggunakan AJAX (Yang & Yang, 2014). Penelitian SSO dengan Load Distribution Method dilakukan oleh Surachai meningkatkan dukungan session baru dan konkuren session sehingga dapat meningkatkan kemampuan SSO(Chitpinityon & Tossa, 2021). Lalu penelitian dengan two-factor authentication dilakukan oleh Bekmezci dengan mengkombinasikan OTP (One time Passwords) dan SSO(Bekmezci et al., 2018). Terdapat juga penelitian SSO dengan menggunakan SAML yang dilakukan oleh Nishioka, Telnoni dan Binu. Pada penelitian Nishioka open source SimpleSAMPphp digunakan untuk membantu menerapkan implementasi memindahkan akun pada banyak SP (Service Provider)(Nishioka & Okabe, 2020b). Lalu pada penelitian Telnoni, SAML digunakan sebagai protocol namun dinilai kurang aman sehingga dikombinasikan dengan speech dan speaker recognition untuk mengurangi dampat ketidakamanan SSO yang dikembangkan(Telnoni et al., 2015). Sedangkan pada penelitian oleh Binu mengusulkan skema berbasis Secure Dynamic-ID menggunakan smart-card yang tidak memerlukan tabel verifikasi dan mengimplementasikan fitur Single Sign On menggunakan protokol SAML, sehingga memungkinkan pengguna untuk menikmati semua fitur MSE(Multi Server Environment) bersama dengan SSO (Binu et al., 2014).

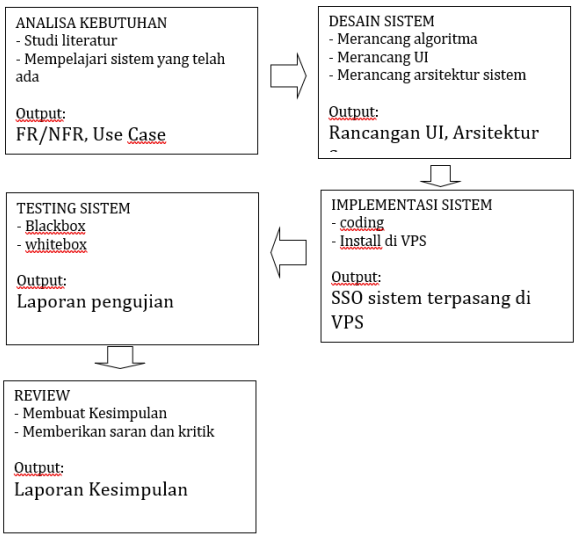
Berdasarkan hasil penelitian kami, terdapat juga jurnal mengenai SSO yang

menggunakan OAuth2 dan OpenID Connect. Penelitian dengan OAuth2 ditulis oleh Hossain yang membahas tentang framework untuk meningkatkan keamanan layanan Single Sign-On (SSO) dengan protokol OAuth, namun pada penelitian ini dibahas juga ancaman-ancaman yang masih bisa terjadi salah satunya adalah resiko implisit session pada IdP(Hossain et al., 2018). Sedangkan penelitian dengan OpenID Connect dilakukan oleh Bellamy menyajikan model berdasarkan prinsip analisis dari metode openID connect yang diterapkan pada lingkup SSO (Bellamy-McIntyre et al., 2011). Pada jurnal ini juga Bellamy menyoroti masalah yang bisa terjadi pada SSO dengan openID seperti malicious provider(idp) dan exploiting redirect.

Dari kedua jurnal tersebut serangan terhadap Idp adalah salah satu ancaman yang sering terjadi pada SSO dengan teknologi openID. Karena itu, pada penelitian ini diajukan teknologi blockchain (NFT) sebagai salah satu solusi untuk masalah tersebut. Meskipun begitu teknologi blockchain juga telah dipakai dalam SSO seperti pada penelitian Arslan (Arslan & Aslan, 2019) dan Matloob (Roy et al., 2021). Namun berbeda dengan penelitian ini yang menggunakan teknologi blockchain-NFT sebagai bukti kepemilikan di IdP, teknologi blockchain pada penelitian Arslan digunakan sebagai user akses manajemen di alat IoT sedangkan teknologi blockchain pada penelitian Matloob digunakan sebagai data distribusi, replikasi, dan juga perbandingan dengan data di RDMS

## METODE

Penelitian ini merupakan penelitian dengan pengembangan perangkat lunak. Oleh karena itu metode penelitian ini digabungkan dengan kaidah dari metode SDLC *atau software development life cycle*. Metode penelitian mengacu pada tahapan metode penelitian dan pengembangan (Research and Development). Prosedur penelitian yang dilakukan disajikan pada Gambar 1 berikut ini. Metode penelitian yang digunakan oleh penulis adalah dengan melakuan study literature terhadap penelitian sebelumnya yang terkait, kemudian dilanjutkan dengan tahapan-tahapan berikut: analisa kebutuhan, desain, konfigurasi dan testing, serta implementasi



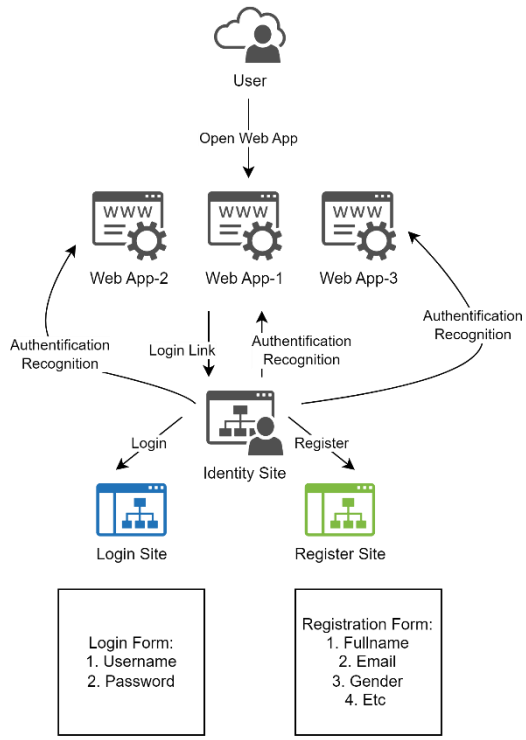

**Gambar 1. Metode Penelitian Dengan SDLC**

## HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk membangun model aplikasi SSO dengan menggunakan OpenID Connect diatas protocol OAuth 2.0. Namun pada implementasinya masih banyak ancaman yang dapat menyerang aplikasi SSO ini salah satunya ancaman penyerangan pada IdP (Identity Provider). Karena itu pada penelitian ini diajukan salah satu cara untuk mencegah hal itu dengan menambahkan NFT sebagai bukti kepemilikan di IdP.

Pembahasan pada pada penelitian ini dimulai dengan menganalisis kebutuhan dari sistem yang akan dibangun. Pada sudut pandang user, ketika memasuki sebuah aplikasi web, login biasanya dilakukan pada aplikasi web tersebut. Namun berbeda dengan konsep SSO. Ketika user akan login ke dalam sistem yang diinginkannya maka user akan di *redirect* ke dalam sebuah website SSO (*identity* site) dengan domain berbeda. Pada website *identity* ini user dapat melakukan login untuk memverifikasi akunnya (biasanya dengan

menginputkan *username* dan *password*). Jika login berhasil maka user akan kembali di *redirect* ke aplikasi web yang diinginkannya, jika tidak maka user akan diminta mengulang username dan password atau bisa juga mengaktifkan fitur lupa password. Sekilas tidak ada perbedaan signifikan pada kegiatan user ini, namun secara metode dan teknologi terdapat perbedaan yang cukup mendasar. Perbedaan yang paling mendasarnya adalah user tidak diperlukan untuk login kembali pada aplikasi dalam lingkungan yang sama. Contohnya pada gambar 2 mengenai arsitektur sistem berdasarkan sudut pandang user, user yang login melalui web app-1 bisa langsung masuk ke web app-2 dan web app-3 tanpa perlu login kembali.




**Gambar 2. Arsitektur Berdasarkan Sudut Pandang User**

Berdasarkan analisis dari penelitian ini, kami menyimpulkan bahwa terdapat 2 hal yang harus dibangun: Mekanisme login dan penerapan NFT pada OpenID dan Oauth2 dengan pembangunan website identity sebagai jalan masuk otentifikasi user.

## 1. Mekanisme login dan penerapan NFT pada OpenID dan Oauth2

Proses login SSO dengan NFT diawali dengan pengguna mengakses aplikasi atau situs web yang terhubung dengan SSO menggunakan protokol OpenID Connect dan OAuth2. Aplikasi atau situs web kemudian mengirimkan permintaan autentikasi ke IDP menggunakan protocol OpenID Connect dan OAuth2.0. IDP lalu menerima permintaan autentikasi dan mengarahkan pengguna ke halaman login IDP. Pengguna kemudian memasukkan kredential login mereka, seperti *username* dan *password,* untuk mengautentikasi diri kepada IDP. Setelah pengguna berhasil diotentikasi, IDP menghasilkan NFT baru yang terenkripsi dan terkait dengan akun IDP pengguna. NFT tersebut disimpan di IDP dan dikirimkan ke aplikasi atau situs web yang melakukan permintaan autentikasi melalui OAuth2.0. Aplikasi atau situs web yang menerima NFT dari IDP kemudian memverifikasinya menggunakan kunci public yang telah didapatkan sebelumnya dari IDP. Jika NFT terverifikasi sebagai bukti kepemilikan IDP yang valid dan keasliannya terjamin, aplikasi atau situs web memberikan akses kepada pengguna. Selama sesi SSO masih aktif, pengguna dapat mengakses aplikasi atau situs web lain yang terhubung dengan SSO dengan menggunakan NFT sebagai bukti otentikasi tambahan. Ketika pengguna ingin logout dari sesi SSO, aplikasi atau situs web mengirimkan permintaan logout ke IDP melalui OAuth2, yang akan mencabut atau menghapus NFT yang terkait dengan sesi tersebut.

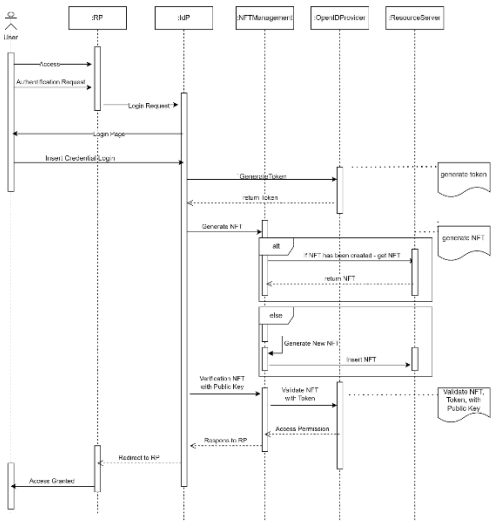
Berdasarkan gambar 3 pengguna yang ingin mengakses sebuah aplikasi yang membutuhkan otentikasi. Aplikasi tersebut berperan sebagai Relying Party (RP) yang ingin memberikan layanan kepada pengguna menggunakan Single Sign-On (SSO).

Pengguna memulai dengan mengakses aplikasi yang menampilkan tampilan awal. Melalui antarmuka aplikasi, pengguna dapat memilih layanan yang ingin diakses. Ketika pengguna memilih

layanan yang membutuhkan otentikasi, aplikasi akan mengirimkan permintaan otentikasi ke Identity Provider (IDP) yang merupakan penyedia identitas pengguna.

Permintaan otentikasi dikirim dalam bentuk protokol OpenID Connect (OIDC) yang menggunakan framework OAuth 2.0. IDP kemudian merespons permintaan dengan mengalihkan pengguna ke halaman login IDP. Pengguna akan diarahkan untuk memasukkan kredensial login, seperti nama pengguna dan kata sandi, pada halaman login IDP.

Setelah pengguna memasukkan kredensial login, IDP memvalidasi dan mengautentikasi pengguna. DP melakukan verifikasi kredensial yang diberikan oleh pengguna dengan menggunakan mekanisme keamanan yang sesuai, seperti hashing dan penyimpanan yang aman. Jika autentikasi berhasil,




**Gambar 3. Proses SSO dengan NFT dan OpenID**

IDP menghasilkan Non-Fungible Token (NFT) baru sebagai bukti kepemilikan IDP. Proses generasi NFT melibatkan komponen NFT Management (NFTM). NFTM bertugas untuk menghasilkan NFT yang unik dan terenkripsi untuk setiap pengguna yang berhasil diautentikasi. NFT ini berisi informasi yang relevan, seperti ID pengguna, waktu kadaluwarsa, dan tanda tangan digital yang digunakan untuk verifikasi.

Algoritma 1. Generate NFT

```
const crypto = require('crypto');
function generateNFT(userData, privateKey) {
  // Convert userData to JSON string
  const jsonData = JSON.stringify(userData);

  // Generate hash value using SHA-256 algorithm
  const hash = crypto.createHash('sha256').update(jsonData).digest('hex');

  // Create digital signature using private key
  const sign = crypto.createSign('RSA-SHA256');
  sign.update(hash);
  const signature = sign.sign(privateKey, 'hex');

  // Create NFT by combining hash value and digital signature
  const nft = hash + signature;

  return nft;
}

// Contoh penggunaan
const userData = {
  id: '12345',
  name: 'John Doe',
  email: 'john.doe@example.com',
  // tambahkan atribut tambahan jika diperlukan
};

const privateKey = 'PRIVATE_KEY_HERE'; // private key IDP (harap disimpan dengan aman)

const nft = generateNFT(userData, privateKey);
console.log('NFT:', nft);
```

Proses algoritmanya menggunakan fungsi generateNFT yang menerima userData sebagai objek data pengguna dan privateKey sebagai kunci privat IDP. Data pengguna kemudian diubah menjadi string JSON dengan JSON.stringify(userData).

Kemudian, menggunakan algoritma hashing SHA-256, dilakukan hashing pada string data untuk menghasilkan nilai hash. Selanjutnya, crypto.createSign digunakan untuk membuat digital signature menggunakan kunci privat IDP. Hash nilai tadi ditandatangani dengan menggunakan sign.sign(privateKey, 'hex'), menghasilkan tanda tangan digital. Terakhir, nilai hash dan tanda tangan digital digabungkan untuk membentuk NFT. NFT inilah yang kemudian dikembalikan sebagai hasil generateNFT.

Setelah NFT dihasilkan, IDP mengirimkan NFT tersebut kepada pengguna sebagai respons atas permintaan otentikasi. NFT dikirimkan dalam bentuk yang terenkripsi dan aman, memastikan kerahasiaan dan integritas data. Pengguna akan menerima NFT sebagai bukti otentikasi yang valid untuk mengakses layanan yang terhubung dengan IDP tersebut.

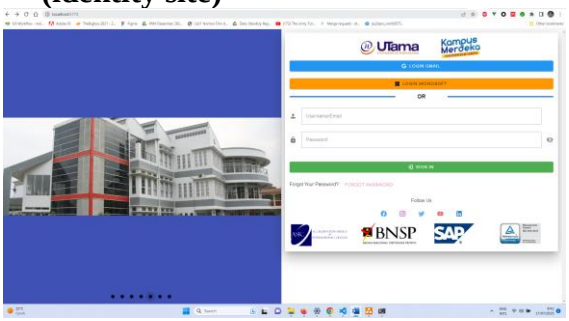
Ketika pengguna ingin mengakses layanan yang membutuhkan otentikasi, pengguna akan mengirimkan permintaan ke Resource Server yang menyediakan layanan tersebut. Permintaan ini mencakup NFT sebagai bukti kepemilikan IDP. Resource Server akan melakukan verifikasi terhadap NFT dengan menggunakan kunci publik yang diperoleh dari OpenID Provider (OIDP).

OIDP bertindak sebagai pihak yang memverifikasi integritas dan keabsahan NFT yang diberikan oleh IDP. OIDP menggunakan kunci publik yang bersifat unik untuk setiap RP yang terdaftar dalam sistemnya. Dengan menggunakan kunci publik ini, OIDP dapat memverifikasi tanda tangan digital yang ada dalam NFT dan memastikan bahwa NFT adalah asli dan belum dimanipulasi.

Setelah NFT terverifikasi, Resource Server memberikan akses kepada pengguna untuk menggunakan layanan yang diminta. Pengguna dapat mulai menggunakan layanan tersebut tanpa perlu memberikan kredensial login lagi. NFT berfungsi sebagai token akses yang terenkripsi dan memiliki masa berlaku tertentu. Jika masa berlaku NFT telah habis, pengguna akan diminta untuk melakukan otentikasi ulang dengan IDP untuk mendapatkan NFT baru.

Dalam konteks ini, pengguna dapat dengan mudah mengakses berbagai layanan yang terhubung dengan IDP tanpa perlu mengingat dan memasukkan kredensial login yang berbeda setiap kali. Dengan menggunakan mekanisme SSO dan NFT sebagai bukti kepemilikan IDP, pengguna dapat mengalami kenyamanan dan efisiensi dalam menjelajahi berbagai aplikasi dan layanan dengan satu kali otentikasi.

## 2. Pembangunan front-end website SSO (identity site)




**Gambar 4. Tampilan UI Website SSO**

Website identity adalah aplikasi yang dipakai sebagai sentral login dari skema aplikasi SSO. Setiap user yang akan melakukan login dari suatu aplikasi maka user akan dialihkan ke website identity ini. Pembangunan website identity ini dirancang memiliki 3 fungsi yaitu proses login, lupa password, dan register.

Pada halaman utama website ini pengguna dapat mendaftar akun baru atau melakukan login jika sudah memiliki akun. Proses pendaftaran akun baru melibatkan pengisian formulir dengan informasi pribadi, seperti nama lengkap, alamat email, dan password yang kuat. Pada proses login pada website identity ini dapat melakukan login dengan beberapa cara, diantaranya dengan menggunakan akun Google, akun Microsoft, atau dengan *username-password* saja. Selain itu jika user lupa akan *password*nya maka terdapat juga fitur lupa *password* yang bisa digunakan

## SIMPULAN

Pada penelitian ini, penerapan NFT (*Non-Fungible Token*) dijadikan sebagai bukti kepemilikan Identity Provider (IDP) dalam Single Sign-On (SSO) dengan protokol OpenID Connect. Kami menggambarkan mekanisme login SSO dengan menggunakan NFT sebagai token akses yang terenkripsi.

Berdasarkan hasil analisis kami, penerapan NFT dalam SSO dengan OpenID Connect dapat memberikan beberapa keuntungan. NFT sebagai bukti kepemilikan IDP memungkinkan pengguna untuk mengakses berbagai layanan dengan login sekali saja, menghindari kebutuhan untuk login ulang pada setiap layanan. Ini meningkatkan efisiensi dan kenyamanan pengguna dalam menjelajahi aplikasi dan layanan yang terhubung dengan IDP. Selain itu, penggunaan NFT yang terenkripsi dan ditandatangani digital signature meningkatkan keamanan dalam mekanisme otentikasi.

Pada pengembangan selanjutnya, penelitian dapat dilakukan untuk mengevaluasi dan menguji keandalan serta skalabilitas dari mekanisme login SSO dengan NFT. Ini dapat melibatkan pengujian dan pengukuran kinerja dalam skenario dengan jumlah pengguna yang besar dan penggunaan yang intensif.

Selain itu, Penelitian lebih lanjut juga dapat fokus pada analisis keamanan yang lebih mendalam terkait dengan penerapan NFT dalam SSO dengan OpenID Connect. Hal ini termasuk pengujian serangan potensial, verifikasi terhadap kerentanan keamanan, dan peningkatan mekanisme keamanan untuk melindungi NFT dan data pengguna. Analisis perbandingan antara SSO dengan NFT dan teknologi SSO lainnya dirasa perlu dilakukan, seperti SAML (*Security Assertion Markup Language*) atau JWT (JSON *Web Tokens*), dapat membantu memahami kelebihan dan kekurangan dari setiap pendekatan dan menentukan pilihan terbaik untuk skenario tertentu.

Dengan penelitian dan pengembangan yang terus berlanjut, penerapan NFT dalam SSO dengan OpenID Connect dapat terus meningkatkan keamanan, kenyamanan, dan efisiensi dalam pengelolaan otentikasi dan akses pengguna di lingkungan digital

## DAFTAR PUSTAKA

Ahammad Karim, & Muhammad Abdullah Adnan. (2019). An OpenID Based Authentication Service Mechanisms for Internet of Things. *2019 IEEE 4th International Conference on Computer and Communication Systems, ICCCS 2019*, 655–659. https://doi.org/10.1109/CCOMS.2019.8821761

Arslan, H., & Aslan, H. (2019). Blockchain based single sign-on support for IoT environments. *27th Signal Processing and Communications Applications Conference, SIU 2019*. https://doi.org/10.1109/SIU.2019.8806439

Asnawi, A. (2022). KESIAPAN INDONESIA MEMBANGUN EKONOMI DIGITAL DI ERA REVOLUSI INDUSTRI 4.0. *Jurnal Ilmiah Indonesia*, *7*(1).

Bekmezci, A. B., Eris, C., & Boluk, P. S. (2018). A multi-layered approach to securing enterprise applications by using TLS, two-factor authentication and single sign-on. *26th IEEE Signal Processing and Communications Applications Conference, SIU 2018*, 1–4. https://doi.org/10.1109/SIU.2018.8404773

Bellamy-McIntyre, J., Luterroth, C., & Weber, G. (2011). OpenID and the enterprise: A model-based analysis of single sign-on authentication. *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*, 129–138.

https://doi.org/10.1109/EDOC.2011.26

Binu, S., Misbahuddin, M., & Raj, P. (2014). A Single Sign on based secure remote user authentication scheme for Multi-Server Environments. *International Conference on Computing and Communication Technologies, ICCCT 2014*. https://doi.org/10.1109/ICCCT2.2014.7066715

Chitpinityon, S., & Tossa, M. (2021). New Approach for Single Sign-on Improvement using Load Distribution Method. *Proceedings - 2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics, RI2C 2021*, 44–47. https://doi.org/10.1109/RI2C51727.2021.9559786

Dissanayake, N., & Diaz, G. (2017). Web-based Applications: Extending the General Perspective of the Service of Web. *10th International Research Conference of KDU (KDU-IRC 2017) on Changing Dynamics in the Global Environment: Challenges and Opportunities*. https://www.researchgate.net/publication/319058851_Web-based_Applications_Extending_the_General_Perspective_of_the_Service_of_Web

Dodanduwa, K., & Kaluthanthri, I. (2018). Role of Trust in OAuth 2.0 and OpenID Connect. *2018 IEEE 9th International Conference on Information and Automation for Sustainability, ICIAfS 2018*. https://doi.org/10.1109/ICIAFS.2018.8913384

Hossain, N., Hossain, M. A., Hossain, M. Z., Sohag, M. H. I., & Rahman, S. (2018). OAuth-SSO: A Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 1575–1578. https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2018.00227

Iskandar, D., & Isnaeni, M. (2019). PENGGUNAAN INTERNET DI KALANGAN REMAJA DI JAKARTA. *Communicare: Journal of Communication Studies*. https://doi.org/https://doi.org/10.37535/101009220222

Jain, K., & Shete, V. V. (2016). Single sign on using bluetooth device. *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, 2016*. https://doi.org/10.1109/INVENTIVE.2016.7830186

Liu, D., Zhang, Z. J., & Zhang, N. (2012). A biometrics-based SSO authentication scheme in telematics. *Proceedings of the 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2012*, 191–194. https://doi.org/10.1109/CYBERC.2012.39

Liu, W., Wang, X., Peng, W., & Xing, Q. (2019). Center-Less Single Sign-On with Privacy-Preserving Remote Biometric-Based ID-MAKA Scheme for Mobile Cloud Computing Services. *IEEE Access*, *7*, 137770–137783. https://doi.org/10.1109/ACCESS.2019.2942987

Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security - An Evaluation of OpenID Connect. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, 251–266.

https://doi.org/10.1109/EUROSP.2017.32

Mladenov, V., Schwenk, J., & Mainka, C. (2016). Do not trust me: Using malicious IdPs for analyzing and attacking single sign-on. *Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016*, 321–336. https://doi.org/10.1109/EUROSP.2016.33

*NFC based mobile single sign-on solution as a chrome extension | IEEE Conference Publication | IEEE Xplore*. (n.d.). Retrieved April 7, 2023, from https://ieeexplore.ieee.org/document/7509508

Nishioka, S., & Okabe, Y. (2020a). Centralized Control of Account Migration at Single Sign-On in Shibboleth. *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1597–1603. https://doi.org/10.1109/COMPSAC48688.2020.00-27

Nishioka, S., & Okabe, Y. (2020b). Centralized Control of Account Migration at Single Sign-On in Shibboleth. *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1597–1603. https://doi.org/10.1109/COMPSAC48688.2020.00-27

Roy, S., Matloob, S., & Mukhopadhyay, D. (2021). On Application of Blockchain to Enhance Single Sign-On (SSO) Systems. *Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021*, 1191–1195. https://doi.org/10.1109/TRUSTCOM53373.2021.00161

Sharma, P., & Sihag, V. K. (2016). Hybrid Single Sign-On Protocol for Lightweight Devices. *Proceedings - 6th International Advanced Computing Conference, IACC 2016*, 679–684. https://doi.org/10.1109/IACC.2016.131

Spoorthi, V., & Sekaran, K. C. (2014). Mobile single sign-on solution for enterprise cloud applications. *1st International Conference on Networks and Soft Computing, ICNSC 2014 - Proceedings*, 273–277. https://doi.org/10.1109/CNSC.2014.6906717

Su, Z., He, Q., Zhang, J., & Li, H. (2013). Research of single sign-on in mobile RFID middleware based on dynamic tokens and WMMP. *Proceedings - 16th IEEE International Conference on Computational Science and Engineering, CSE 2013*, 1191–1194. https://doi.org/10.1109/CSE.2013.177

Takahashi, H., & Lakhani, U. (2021). Voting blockchain for High Security NFT. *2021 IEEE 10th Global Conference on Consumer Electronics, GCCE 2021*, 358–361. https://doi.org/10.1109/GCCE53005.2021.9621968

Telnoni, P., Munir, R., & Rosmansyah, Y. (2015). SAML single sign-on protocol development using combination of speech and speaker recognition. *Proceedings - 2014 International Conference on Advanced Informatics: Concept, Theory and Application, ICAICTA 2014*, 299–304. https://doi.org/10.1109/ICAICTA.2014.7005958

Yang, T. J., & Yang, X. J. (2014). Method of single sign-on for independent web systems based on AJAX. *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, ICCSNT 2013*, 310–314. https://doi.org/10.1109/ICCSNT.2013.6967119

Zhang, L., Ning, H. Y., Du, Y. Y., Cui, Y. X., & Yang, Y. (2016). A new identity authentication scheme of single sign on for multi-database. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, *0*, 458–461. https://doi.org/10.1109/ICSESS.2016.7883108