

## PENGEMBANGAN *SINGLE SIGN ON (SSO)* MENGGUNAKAN TEKNOLOGI *MAGIC LINK* DI UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMMI)

Ruswandi<sup>1</sup>, Franciskus Antonius Alijoyo<sup>2</sup>

<sup>1,2</sup>Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Jl. Ir. Juanda 96 Bandung 40132

<sup>1</sup>[sukabumikode@gmail.com](mailto:sukabumikode@gmail.com), <sup>2</sup>[franciskus.antonius.alijoyo63@gmail.com](mailto:franciskus.antonius.alijoyo63@gmail.com)

### Abstract

*The use of information systems in educational institutions and companies is rapidly evolving, but often accompanied by complex account management challenges, forcing users to remember numerous accounts. Although conventional Single Sign-On (SSO) systems such as Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS), and Keycloak can address this issue, cost and high human resource requirements are obstacles. Muhammadiyah University of Sukabumi (UMMI), a private university in Sukabumi, faces these challenges, with dozens of standalone information systems that are not yet integrated. As a solution to this problem, the use of magic link login with JSON Web Token (JWT) is proposed. This enables easier and more affordable SSO implementation, even for institutions with limited resources. The research involves three systems most relevant to UMMI students: Academic Information System, e-Learning, and Library System. Based on testing, students only need to authenticate once in the Academic Information System to directly access e-Learning and the Library System through special links (magic links), without needing to authenticate again. This development is implemented directly into the existing systems without the need for additional servers or new user management systems, making it a highly effective and efficient solution to address previous issues.*

**Keywords :** *single sign on, sso, magic link, json web token, jwt*

### Abstrak

Penggunaan sistem informasi di institusi pendidikan dan perusahaan berkembang pesat, tetapi seringkali diikuti oleh tantangan manajemen akun yang kompleks, memaksa pengguna untuk mengingat banyak akun. Meskipun *Single Sign On (SSO)* konvensional seperti *Lightweight Directory Access Protocol (LDAP)*, *Central Authentication Service (CAS)* dan *Keycloak* dapat mengatasi masalah ini, biaya dan kebutuhan SDM yang tinggi menjadi kendala. Universitas Muhammadiyah Sukabumi (UMMI), sebuah perguruan tinggi swasta di Sukabumi, mengalami kendala tersebut, dimana sudah terdapat belasan sistem informasi yang masih bersifat standalone dan belum terintegrasi. Sebagai solusi atas permasalahan tersebut, penggunaan *magic link login* dengan *JSON Web Token (JWT)* diusulkan. Ini memungkinkan implementasi SSO yang lebih mudah dan terjangkau, bahkan bagi institusi dengan sumber daya terbatas. Penelitian melibatkan tiga sistem yang paling relevan dengan mahasiswa UMMI, yakni Sistem Informasi Akademik, e-Learning, dan Sistem Perpustakaan. Berdasarkan pengujian, mahasiswa hanya perlu melakukan proses otentikasi di Sistem Informasi Akademik untuk dapat langsung mengakses e-Learning dan Sistem Perpustakaan melalui tautan khusus (*magic link*), tanpa perlu melakukan proses otentikasi lagi. Pengembangan ini diimplementasikan langsung pada sistem yang sudah berjalan tanpa memerlukan penambahan server atau sistem manajemen pengguna baru, sehingga menjadi solusi yang sangat efektif dan efisien dalam menangani permasalahan sebelumnya.

**Kata kunci :** *single sign on, sso, magic link, json web token, jwt*

### 1. PENDAHULUAN

Di era dimana teknologi digital berkembang dengan cepat, penggunaan sistem informasi telah menjadi bagian integral dari operasional berbagai

institusi pendidikan dan perusahaan. Kemajuan teknologi telah memungkinkan adopsi sistem informasi yang beragam untuk meningkatkan efisiensi dan produktivitas[1]. Namun, seiring

bertambahnya jumlah sistem informasi yang digunakan, muncul tantangan dalam manajemen akun yang kompleks bagi pengguna. Pengguna sering kali harus mengingat banyak kredensial untuk mengakses berbagai sistem, menyebabkan ketidaknyamanan, kerumitan, serta dapat menghambat produktivitas dan meningkatkan risiko organisasi untuk tumbuh secara optimal[2].

Di sisi lain, pendekatan umum dalam mengatasi masalah manajemen akun, seperti menggunakan *Single Sign On (SSO)*[3], seringkali dihadapkan pada kendala biaya yang tinggi[4] dan kebutuhan akan SDM yang berkualifikasi. Hal ini mengakibatkan sulitnya implementasi solusi *SSO* bagi institusi dengan anggaran terbatas atau kurangnya tenaga ahli di bidang teknologi informasi.

Universitas Muhammadiyah Sukabumi (UMMI), sebuah institusi perguruan tinggi di Jawa Barat dengan jumlah mahasiswa lebih dari 4.500, mengalami kendala tersebut, dimana sudah terdapat tiga belas sistem informasi yang berkaitan dengan mahasiswa yang masih bersifat *standalone* dan belum terintegrasi. Mahasiswa diharuskan untuk memasukan NIM dan sandi untuk bisa masuk ke setiap sistem, sehingga ini sangat merepotkan dan tidak efisien.

Penelitian sebelumnya mengenai pengembangan *SSO* menggunakan berbagai teknologi seperti *Lightweight Directory Access Protocol (LDAP)*, *Central Authentication Service (CAS)* hingga *Keycloak*[5]. Seperti yang dilakukan oleh R. G. Jatsuma[6] yang meneliti penggunaan *Java Open Single Sign-On (JOSSO)* dan Sistem Operasi *TurnKey OpenLDAP* telah memungkinkan mahasiswa untuk masuk ke beberapa sistem kampus XYZ dengan satu kali proses otentikasi, penelitian oleh A. Kurnianto dkk.[7] yang menerapkan *SSO* dengan metode *LDAP* di PT Unichem telah memungkinkan pegawai untuk bisa mengakses beberapa aplikasi dengan satu kali proses otentikasi, penelitian oleh M. Kondo[8] yang mengimplementasikan *Central Authentication Service (CAS)* di Politeknik Negeri Manado memungkinkan pengguna memiliki satu akun untuk mengakses beberapa aplikasi secara langsung, penelitian oleh I.Suryadi[9] yang mengintegrasikan *CAS* dengan *Freeradius* sebagai *SSO* telah memungkinkan pengguna yang masuk ke portal *SSO* dapat mengakses semua web yang ada, penelitian oleh M. A. Saputri[10] yang mengimplementasikan *SSO* menggunakan *keycloak* di STMIK Widya Cipta Dharma telah memungkinkan pengguna untuk mengakses beragam layanan situs web dan aplikasi hanya dengan menggunakan satu kredensial saja, dan penelitian oleh W. Hermawan[11] yang

mengintegrasikan *keycloak* dengan *public key infrastruktur* dalam sistem pemerintahan berbasis elektronik di Indonesia telah memungkinkan pengguna untuk masuk ke berbagai sistem tidak lagi menggunakan kata sandi, tetapi menggunakan *Mutual TLS* yang memanfaatkan *Public Key Infrastructure (PKI)*.

Berdasarkan penelitian sebelumnya, diketahui bahwa telah ada banyak solusi untuk menangani masalah manajemen akun. Namun, semua teknologi tersebut memerlukan anggaran besar dan kualifikasi SDM yang tinggi, sehingga tidak semua institusi atau perusahaan dapat mengimplementasikannya.

Sebagai tanggapan terhadap tantangan ini, penulis mengusulkan solusi alternatif yang inovatif dan terjangkau melalui penggunaan teknologi *magic link* dengan memanfaatkan *JSON Web Token (JWT)*. *Magic link* adalah sebuah tautan khusus yang berisi *token* yang bisa digunakan untuk proses otentikasi[12], sedangkan *JWT* merupakan standar terbuka (RFC 7519) yang menetapkan metode yang sederhana dan mandiri untuk mengirimkan informasi secara aman antara pihak-pihak sebagai objek *JSON*. [13]. Berbeda dengan pendekatan penelitian lain yang menggunakan *magic link technology* sebagai metode otentikasi tanpa kata sandi (*passwordless*)[14][12], penelitian ini mempertahankan kebutuhan akan sandi saat mahasiswa pertama kali masuk, tetapi cukup dengan satu kali melakukan otentikasi, mahasiswa sudah bisa mengakses sistem lainnya tanpa perlu memasukan NIM dan kata sandi kembali.

Penggunaan *JWT* saat ini telah menjadi hal lumrah dalam mengamankan *RESTful web service*[15]. *RESTful API* merupakan jalur komunikasi yang memfasilitasi pertukaran informasi antara dua sistem komputer melalui internet dengan aman[16]. Seperti dalam penelitian yang dilakukan oleh Adam, S. I. dkk. dengan judul "Implementasi Layanan *Web RESTful* pada Sistem Informasi Unklab Menggunakan *JSON Web Token (JWT)*"[17], penelitian oleh Utama, J. S., & Indriyanti, A. D.[18], dan penelitian oleh Pudoli, A., dkk.[19] telah memberikan gambaran tentang manfaat penggunaan *JWT*. Namun, implementasi *JWT* untuk digunakan sebagai *SSO* menggunakan teknologi *magic link* belum pernah diteliti.

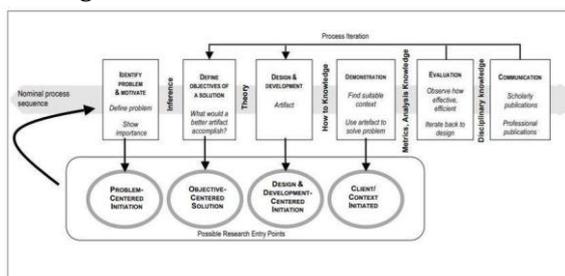
Solusi ini dapat memberikan kemudahan akses ke berbagai sistem informasi dengan hanya melakukan satu kali proses otentikasi di sistem utama, kemudian mengakses sistem-sistem lainnya menggunakan tautan yang tersedia di sistem utama. Pendekatan baru ini diharapkan dapat menjadi solusi yang efektif dalam

meningkatkan pengelolaan akun dan akses sistem informasi pada berbagai tingkatan institusi dan perusahaan tanpa mengurangi aspek keamanan[20].

## 2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan adalah *Design-Science Research Methodology (DSRM)*, yang diadaptasi dari kerangka kerja yang dikemukakan oleh Ken Peffers, dkk.[21]. DSRM menggabungkan berbagai prosedur, prinsip, dan praktik untuk menghasilkan solusi yang konsisten dengan tujuan penelitian, dengan penekanan pada proses literatur yang cermat. DSRM menawarkan panduan proses yang terstruktur untuk melakukan penelitian dan memberikan kerangka kerja konseptual untuk menafsirkan serta mengevaluasi hasil temuan.

Proses DSRM terdiri dari enam langkah utama: identifikasi masalah dan motivasi, perumusan tujuan solusi, desain dan pengembangan, demonstrasi, evaluasi, dan komunikasi. Tahapan DSRM ini dapat dilihat dalam gambar dibawah ini:



Gambar 1. DSRM[21]

### 2.1. Problem Identification and Motivation

Langkah awal penelitian ini melibatkan identifikasi masalah terkait keberadaan banyak sistem informasi yang berdiri sendiri di Universitas Muhammadiyah Sukabumi (UMMI) dan belum terintegrasi. Permasalahan yang muncul mencakup beberapa aspek: pertama, proses akses yang merepotkan ke berbagai sistem yang berbeda, memaksa pengguna untuk melakukan proses masuk berkali-kali; kedua, risiko lupa kata sandi pada beberapa sistem karena variasi yang digunakan; ketiga, kebutuhan untuk mengubah semua kata sandi di semua sistem jika ingin menyamakan semuanya; dan keempat, penggunaan teknologi SSO umum seperti *LDAP*, *CAS*, *Keycloak* dan lainnya belum memungkinkan diimplementasikan karena sumber daya terbatas. Motivasi di balik penelitian

ini adalah untuk mengatasi kesulitan tersebut dengan memungkinkan mahasiswa untuk mengakses berbagai sistem dengan satu proses autentikasi.

### 2.2. Define the Objectives for a Solution

Setelah mengidentifikasi masalah, langkah selanjutnya adalah mendefinisikan tujuan dari solusi yang akan dikembangkan. Tujuan utama penelitian ini adalah merancang dan mengimplementasikan sebuah solusi pengembangan SSO yang lebih mudah dan terjangkau, bahkan bagi institusi dengan sumber daya terbatas. Sebagai solusi, penggunaan teknologi *magic link* dengan memanfaatkan *JWT* telah dipilih untuk diteliti dan diimplementasikan guna menyelesaikan permasalahan ini.

### 2.3. Design and Development

Berdasarkan identifikasi masalah dan pemahaman domain, dilakukan perancangan dan pengembangan mengembangkan solusi berupa penggunaan teknologi *magic link* dengan memanfaatkan *JSON Web Token (JWT)*. *JWT* dipilih karena kemudahannya dalam penggunaan dan didukung oleh hampir semua bahasa pemrograman.

Dalam proses pengembangan ini, tiga sistem yang terkait dengan mahasiswa diambil sebagai contoh, yaitu Sistem Informasi Akademik, e-Learning, dan Sistem Perpustakaan.

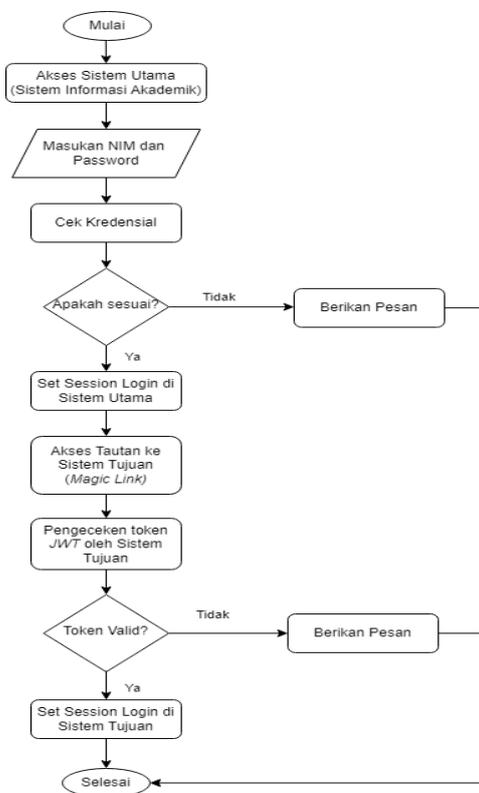
Agar dapat memahami rancangan solusi yang dikembangkan, penting untuk memahami kondisi penelitian, skema penggunaan SSO umum dengan biaya pengembangan yang tinggi, dan solusi baru yang dikembangkan. Kondisi sebelum penelitian seperti pada Gambar 2, yang mana mahasiswa harus memasukan NIM dan password ketika hendak mengakses sistem informasi tertentu.



	UxNjIzOTAyMn0.aaKFYEjKTmklXVf5phcqST8bKq6qpxQvpqm0XHnync
Sistem Perpustakaan	<a href="https://opac-perpustakaan.ummi.ac.id/magic-link?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEwMDAiLCJlbWFpbCI6InN1a2FidW1pa29kZUBnbWVpbC5jb20iLCJyb2RlIjoic3R1ZGVudCIsInN5c3R1bSI6ImxpYnJhcnkiLCJpYXQiOiE1MTYyMzkwMjJ9.tlVrEA6dqTBWuAeLDh_pi0J3TT1jAmUW1a5Tx_9jZY4">https://opac-perpustakaan.ummi.ac.id/magic-link?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEwMDAiLCJlbWFpbCI6InN1a2FidW1pa29kZUBnbWVpbC5jb20iLCJyb2RlIjoic3R1ZGVudCIsInN5c3R1bSI6ImxpYnJhcnkiLCJpYXQiOiE1MTYyMzkwMjJ9.tlVrEA6dqTBWuAeLDh_pi0J3TT1jAmUW1a5Tx_9jZY4</a>

Dalam Tabel 1, terdapat kolom *Magic Link* yang berisi tautan ke sistem yang dituju. Parameter *token* pada tautan tersebut berisi *token* dalam format *JWT*. Sistem yang dituju akan melakukan validasi terhadap *token* yang dikirim. Jika *token* dinyatakan *valid*, sistem akan membuat sesi baru berdasarkan data dalam *token* tersebut, dan mahasiswa dianggap telah berhasil masuk ke sistem. Namun, jika *token* dinyatakan tidak valid, sistem akan menampilkan pemberitahuan.

Proses dari mulai mahasiswa melakukan proses *login* di sistem utama hingga masuk ke sistem lainnya menggunakan teknologi *magic link* login seperti pada Gambar 6.



Gambar 6: Diagram Alir Akses Sistem Lainnya Menggunakan Teknologi *Magic Link*

## 2.4. Demonstration

Solusi yang telah dikembangkan kemudian diimplementasikan dalam lingkungan sistem yang sebenarnya. Proses ini melibatkan demonstrasi fungsionalitas *SSO* menggunakan teknologi *magic link* yang telah dirancang, dengan melakukan pengujian terhadap Sistem Informasi Akademik sebagai sistem utama (<https://siak.ummi.ac.id>), e-Learning (<https://lms.ummi.ac.id>), dan Sistem Perpustakaan (<https://opac-perpustakaan.ummi.ac.id>) sebagai sistem yang bisa diakses tanpa perlu memasukan NIM dan kata sandi kembali. Demonstrasi ini bertujuan untuk menunjukkan efektivitas pengembangan *SSO* menggunakan teknologi *magic link*.

## 2.5. Evaluation

Setelah implementasi, evaluasi dilakukan terhadap kinerja dan efektivitas penggunaan *magic link*. Proses evaluasi ini melibatkan penyebaran angket kepada mahasiswa untuk mendapatkan tanggapan terhadap pengembangan *SSO* menggunakan teknologi *magic link* yang telah diimplementasikan.

Instrumen angket evaluasi ini terdiri dari lima pertanyaan, dan pengukuran *usability*-nya menggunakan *System Usability Scale (SUS)*[22].

## 2.6. Communication

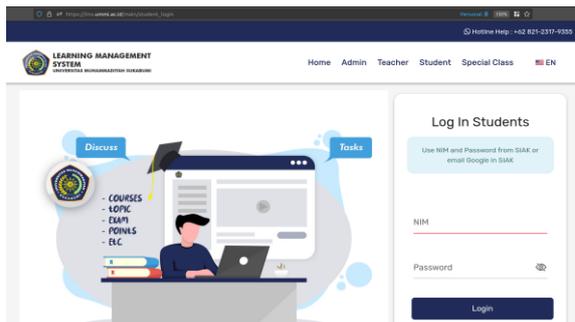
Hasil penelitian dan evaluasi yang telah dilakukan kemudian disampaikan kepada pihak terkait, baik itu manajemen UMMI maupun sivitas akademik lainnya. Komunikasi ini digunakan demi memberikan pemahaman yang lebih akurat tentang manfaat dan efektivitas dari penerapan *magic link* yang telah dikembangkan serta memperoleh masukan dan umpan balik untuk perbaikan dan pengembangan lebih lanjut.

## 3. HASIL DAN PEMBAHASAN

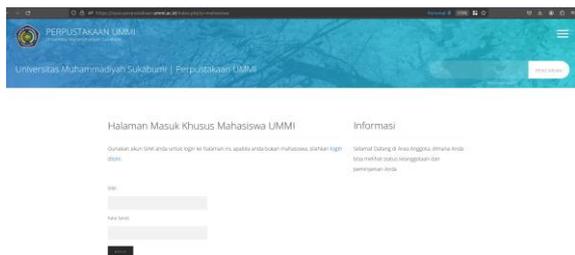
Berdasarkan perencanaan yang telah dipaparkan pada bagian sebelumnya, maka bisa dilakukan uji coba lebih lanjut untuk mendapatkan hasil yang diinginkan. Uji coba dilakukan dengan membuka ketiga sistem dan diarahkan ke halaman *login*.



Gambar 7. Halaman Masuk Ke Sistem Informasi Akademik Yang Menjadi Sistem Utama (<https://siak.ummi.ac.id>)



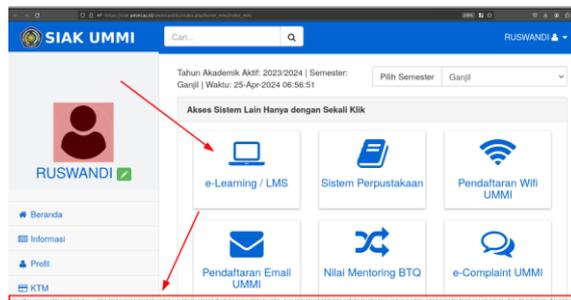
Gambar 8. Halaman Masuk Ke e-Learning (<https://lms.ummi.ac.id>)



Gambar 9. Halaman Masuk Ke Sistem Perpustakaan (<https://opac-perpustakaan.ummi.ac.id>)

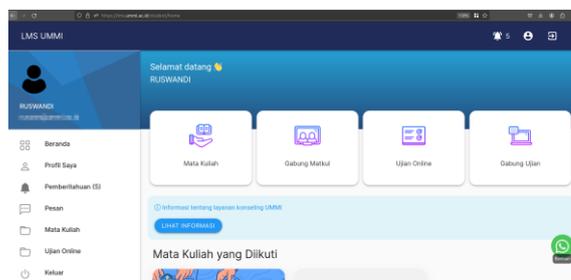
Akses masuk ke sistem lainnya (selain Sistem Informasi Akademik) tetap disediakan menggunakan NIM dan *password*, karena membutuhkan waktu dan sosialisasi supaya bisa diimplementasikan sepenuhnya.

Setelah semua halaman terbuka, demonstrasi dilanjutkan dengan masuk ke sistem utama, yaitu Sistem Informasi Akademik. Setelah berhasil masuk, mahasiswa akan dihadapkan dengan halaman yang menampilkan beberapa menu akses ke sistem lain hanya dengan sekali klik. Ketika kursor diarahkan ke menu atau tulisan e-Learning atau LMS, di bagian bawah layar akan muncul URL yang merupakan *magic link* untuk langsung masuk ke e-Learning seperti yang terlihat pada Gambar 10.



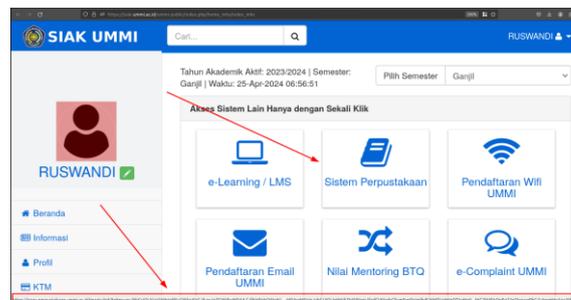
Gambar 10. Akses Ke e-Learning Yang Menggunakan *Magic Link*

Ketika menu atau tulisan "e-Learning/ LMS" diklik, mahasiswa akan diarahkan langsung ke e-Learning seperti yang terlihat pada Gambar 11. *Tab browser* yang menampilkan halaman *login* e-Learning, seperti pada Gambar 8, ketika diperbarui akan langsung mengarah ke halaman beranda mahasiswa seperti pada Gambar 11.

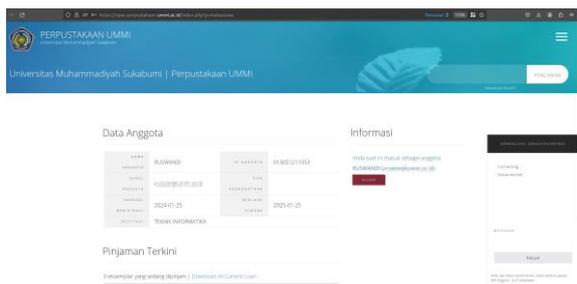


Gambar 11. Halaman Beranda e-Learning Mahasiswa Yang Langsung Bisa Diakses Setelah Meng-Klik Tautan *Magic Link* Di Sistem Informasi Akademik

Demonstrasi berikutnya dilakukan dengan mengklik opsi atau tulisan "Sistem Perpustakaan" pada beranda Sistem Informasi Akademik setelah proses otentikasi atau *login* sebelumnya telah dilakukan. Ketika menu atau tulisan "Sistem Perpustakaan" tersebut di klik (seperti yang terlihat pada Gambar 12), mahasiswa akan diarahkan langsung ke Sistem Perpustakaan dan masuk seperti pada Gambar 13..



Gambar 12. Akses Ke Sistem Perpustakaan Yang Menggunakan *Magic Link*



Gambar 13. Halaman Beranda e-Learning Mahasiswa Yang Langsung Bisa Diakses Setelah Meng-Klik Tautan *Magic Link* Di Sistem Informasi Akademik

Dengan dilakukannya demonstrasi sekaligus pengujian terhadap ketiga sistem tersebut, proses implementasi *magic link* dapat dianggap berhasil. Sehingga bisa disimpulkan bahwa penerapan teknologi *magic link* telah berhasil menjadi alternatif *SSO* karena memungkinkan mahasiswa untuk masuk ke dua sistem lain tanpa harus memasukkan NIM dan kata sandi lagi, karena proses otentikasi telah dilakukan di Sistem Informasi utama. Ketika mahasiswa mengakses halaman beranda Sistem Informasi Akademik yang menampilkan daftar sistem lain yang dapat diakses dengan satu klik seperti yang terlihat pada Gambar 10, di latar belakang sistem terjadi pembuatan *token* menggunakan *JWT* untuk setiap sistem informasi yang terdaftar di beranda. Token yang dibuat berisi beberapa data unik yang dapat digunakan sebagai acuan saat melakukan proses pengecekan dan penentuan sesi di sistem yang dituju. Data unik tersebut berupa id, email, code, role dan system.

Sistem yang dituju yang menerima parameter *token* seperti yang tercantum dalam Tabel 1 akan melakukan proses validasi terhadap *token* tersebut. Validasi dapat dilakukan dengan berbagai metode sesuai yang ditentukan oleh sistem utama, seperti menggunakan *secret key*, *RSA key*[23], *EdDSA/Ed25519 signature*[24], dan metode lainnya. Pada demonstrasi dan uji coba ini, digunakan metode yang paling sederhana, yaitu menggunakan *secret key*. Setelah token dinyatakan *valid*, sistem tujuan akan mengecek *database* berdasarkan data unik yang diperoleh dari token. Dalam percobaan ini, dilakukan dengan menggunakan parameter *code* yang mengindikasikan NIM mahasiswa. Karena sebelumnya NIM telah dipastikan terdaftar (karena proses masuk sebelumnya dilakukan secara manual dengan memasukkan NIM dan kata sandi), maka mahasiswa dengan NIM tersebut dianggap berhasil masuk ke sistem tujuan.

Peneliti melakukan survei yang diikuti oleh 136 mahasiswa (sekitar 3% dari total populasi)

dengan lima pertanyaan. Dari rekapitulasi jawaban, dapat disimpulkan bahwa seluruh responden memberikan respon positif terhadap implementasi *magic link* ini. Instrumen pertanyaan dapat dilihat pada Tabel 2.

TABEL II. INSTRUMEN *SYSTEM USABILITY SCALE (SUS)*

KODE	PERTANYAAN PADA KUESIONER
R1	Saya menilai akses ke sistem lain menjadi lebih mudah dengan adanya <i>magic link</i>
R2	Saya menilai bahwa teknologi <i>magic link</i> bisa menggantikan proses otentikasi sebelumnya
R3	Saya menilai bahwa implementasi <i>magic link</i> ini bisa meningkatkan efektifitas dan efisiensi dalam mengakses sistem di lingkungan kampus
R4	Saya menilai teknologi <i>magic link</i> ini perlu diimplementasikan terhadap semua sistem di lingkungan kampus
R5	Saya menyarankan teknologi <i>magic link</i> ini untuk diimplementasikan di instansi lain yang membutuhkan

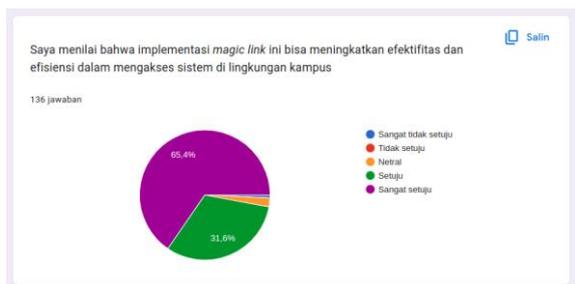
Hasil survei dapat dilihat pada Gambar 14, 15 dan 16, 17 dan 18.



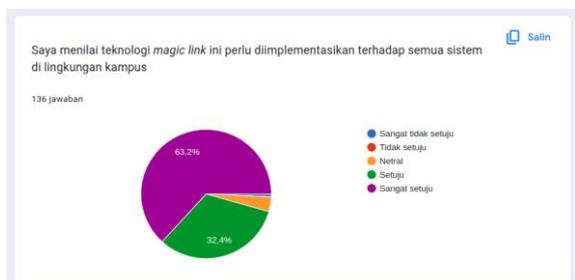
Gambar 14. Hasil Survei Pertanyaan Pertama



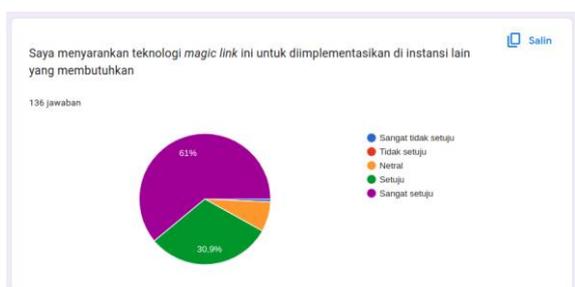
Gambar 15. Hasil Survei Pertanyaan Kedua



Gambar 16. Hasil Survei Pertanyaan Ketiga



Gambar 17. Hasil Survei Pertanyaan Keempat



Gambar 18. Hasil Survei Pertanyaan Kelima

Berdasarkan rekapitulasi keseluruhan hasil survei tersebut, 0,7% memilih sangat tidak setuju, 3,8% memilih netral, 31% memilih setuju, dan 65% memilih sangat setuju. Dengan demikian, dapat disimpulkan bahwa proses implementasi teknologi *magic link* ini berhasil dan memberikan manfaat yang signifikan bagi mahasiswa.

#### 4. KESIMPULAN DAN SARAN

Penelitian ini membahas pengembangan *Single Sign On (SSO)* menggunakan teknologi *magic link* dengan memanfaatkan *JSON Web Token (JWT)* serta implementasinya di Universitas Muhammadiyah Sukabumi (UMMI). Berdasarkan serangkaian penelitian yang telah dilakukan, penggunaan pengembangan *SSO* teknologi *magic link* ini dianggap berhasil, karena mahasiswa hanya perlu melakukan proses otentikasi di Sistem Informasi Akademik untuk dapat langsung mengakses e-Learning dan Sistem Perpustakaan melalui tautan khusus (*magic link*), tanpa perlu melakukan proses otentikasi lagi. Pengembangan

ini diimplementasikan langsung pada sistem yang sudah berjalan tanpa memerlukan penambahan server atau sistem manajemen pengguna baru, sehingga menjadi solusi yang sangat efektif dan efisien, tidak memerlukan biaya besar dan kualifikasi SDM IT yang tinggi. Namun, kelemahan penggunaan teknologi *magic link* sebagai *SSO* adalah ketidakmampuannya mendukung proses *Single Sign-Out*, yang memerlukan pengguna untuk *logout* secara terpisah dari setiap sistem yang diakses sebelumnya.

Sebagai rekomendasi untuk penelitian selanjutnya, disarankan untuk melakukan studi lebih lanjut guna mencari solusi yang memungkinkan implementasi *Single Sign-Out*. Dengan demikian, pengguna dapat keluar dari seluruh sistem yang telah diakses hanya dengan satu kali proses *logout*, sehingga bisa meningkatkan efisiensi dan kenyamanan penggunaan sistem.

#### 5. UCAPAN TERIMA KASIH

Ucapan terima kasih ini disampaikan kepada keluarga, STMIK LIKMI, Universitas Muhammadiyah Sukabumi (UMMI), serta rekan satu kelas yang telah mendukung dalam melakukan penelitian, sehingga jurnal ini bisa tersusun dengan seksama.

#### Daftar Pustaka:

- [1] A. P. Kharismaputra, F. W. Rizkyana, and A. Susanti, "Sistem Informasi Administrasi Perkantoran: Meningkatkan Efisiensi dan Produktivitas," *Bus. Account. Educ. J.*, vol. 3, no. 3, pp. 402–407, 2022.
- [2] F. A. Alijoyo and Y. Munawar, "Faktor yang mempengaruhi maturitas manajemen risiko organisasi di Indonesia," *Bina Ekon.*, vol. 23, no. 1, pp. 67–79, 2019.
- [3] I. K. D. Senapartha, "Implementasi Single Sign-On Menggunakan Google Identity, REST dan OAuth 2.0 Berbasis Scrum," *J. Tek. Inform. dan Sist. Inf.*, vol. 7, no. 2, pp. 307–320, 2021.
- [4] J. Moore, V. Oprica, and D. Gallerizzo, "Why single sign-on is so expensive and what you can do to reduce costs," *J. Digit. \& Soc. Media Mark.*, vol. 5, no. 3, pp. 280–290, 2017.
- [5] D. N. Divyabharathi and N. G. Cholli, "A review on identity and access management server (keycloak)," *Int. J. Secur. Priv. Pervasive Comput.*, vol. 12, no. 3, pp. 46–53, 2020.
- [6] R. G. Jatsuma, "Penerapan Sistem Single Sign On (SSO) Pada Kampus XYZ Berbasis Lightweight Directory Access Protocol

- (LDAP)," *J. Teknol. Pint.*, vol. 2, no. 6, 2022.
- [7] A. Kurnianto, D. H. Sulaksono, and A. Rachman, "Penerapan Single Sign on (Sso) Pada Keamanan Jaringan Dengan Metode Lightweight Directory Access Protocol (Ldap) Di Pt Unichem," *KERNEL J. Ris. Inov. Bid. Inform. dan Pendidik. Inform.*, vol. 3, no. 1, pp. 20–26, 2022.
- [8] M. Kondo, T. Saroinsong, and A. Polii, "Single Sign On (SSO) System with Application of Central Authentication Service (CAS) at Manado State Polytechnic," no. January 2022, pp. 698–702, 2023, doi: 10.5220/0011863100003575.
- [9] I. Suryadi, "Integrasi Central Authentication Service (Cas) Dengan Freeradius Sebagai Single-Sign-on," *Electrician*, vol. 16, no. 1, pp. 20–30, 2022, doi: 10.23960/elc.v16n1.2206.
- [10] M. A. Saputri, "IMPLEMENTASI SINGLE SIGN ON (SSO) MENGGUNAKAN KEYCLOAK PADA SISTEM INFORMASI STMIK WIDYA CIPTA DHARMA," STMIK Widya Cipta Dharma, 2023.
- [11] W. Hermawan, "Single Sign On Using Keycloak Integrated Public Key Infrastructure for User Authentication In Indonesia's Electronic Based Government System," *Adv. Sustain. Sci. Eng. Technol.*, vol. 5, no. 2, p. 230204, 2023.
- [12] I. Matiushin and V. Korkhov, "Passwordless Authentication Using Magic Link Technology," in *CEUR Workshop Proceedings*, 2021, pp. 434–438.
- [13] P. Mahindraka, "Insights of JSON Web Token," *Int. Int. J. Recent Technol. Eng. ISSN*, pp. 2277–3878, 2020.
- [14] V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "A comprehensive study on passwordless authentication," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 2022, pp. 1266–1275.
- [15] C. Pautasso and E. Wilde, "RESTful web services: principles, patterns, emerging technologies," in *Proceedings of the 19th international conference on World wide web*, 2010, pp. 1359–1360.
- [16] F. Amalia, I. W. A. Arimbawa, and R. Afwani, "Implementasi Restful Api Pada Pengembangan Aplikasi If-Ku Berbasis Android," *J. Inform. dan Rekayasa Elektron.*, vol. 2, no. 1, pp. 38–45, 2019.
- [17] S. I. Adam, J. H. Moedjahedy, and J. Maramis, "RESTful Web Service Implementation on Unklab Information System Using JSON Web Token (JWT)," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 2020, pp. 1–6.
- [18] J. S. Utama and A. D. Indriyanti, "Pengamanan Restful API Web Service Menggunakan Json Web Token (Studi Kasus: Aplikasi Siakadu Mobile Unesa)," *J. Emerg. Inf. Syst. Bus. Intell.*, vol. 4, no. 1, pp. 8–17, 2023.
- [19] A. Pudoli, Y. Yulianawati, and I. Suwandi, "Implementasi Web Service Restful Dengan Autentikasi JSon Web Token Berbasis Web dan Android," *Acad. J. Comput. Sci. Res.*, vol. 5, no. 2, pp. 95–103, 2023.
- [20] A. Pathak, T. Patil, S. Pawar, P. Raut, and S. Khairnar, "Secure authentication using zero knowledge proof," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 2021, pp. 1–8.
- [21] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007.
- [22] Intyanto, G. W., Ranggianto, N. A., & Octaviani, V. (2021). Pengukuran Usability pada Website Kampus Akademi Komunitas Negeri Pacitan Menggunakan System Usability Scale (SUS). *Walisongo Journal of Information Technology*, 3(2), 59-68.
- [23] M. Malvin and C. Safitri, "JSON Web Token Leakage Avoidance Using Token Split and Concatenate in RSA256," *Indones. J. Comput. Eng. Des.*, vol. 5, no. 1, pp. 43–56, 2023.
- [24] A. Alkhulaifi and E.-S. M. El-Alfy, "Exploring lattice-based post-quantum signature for JWT authentication: review and case study," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–5.