Inovan Publisher

Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan

| ISSN (Online) 3064-5883 |

DOI: 10.63217/fibonacci.v2i1.256

Implementasi *Multi-Faktor Authentication*, *Single Sign-on* dan *Role-Based Access Contro*l dalam Keamanan Sistem Informasi (Studi Literature Review)

Ahmad Fauzi[1], Inqilaf Nur Aprilla[2], Nabilah Fauziyyah[3], Naila Fazriyanti Bachtiar[4]

[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, inqilafaprilla@gmail.com
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, nabilahfauziyyah941@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, nailafazriyanti.kuliah@gmail.com

Corresponding Author: achmad.fauzi@dsn.ubharajaya.ac.id [1]

Abstract: *This study discusses the effectiveness of Multi-Factor Authentication (MFA), Single Sign-On (SSO), and Role-Based Access Control (RBAC) as the main mechanisms for improving information system security. Through a literature study sourced from journals, books, and proceedings, this study assesses the ability of these three methods to protect data and prevent unauthorized access. The results of the study show that MFA adds a layer of verification that can reduce the risk of account hacking, SSO improves authentication efficiency with a single login for various services, and RBAC regulates access rights in a structured manner based on user roles. The integration of these three methods has been proven to build a stronger and more adaptive security architecture. This study confirms that the implementation of MFA, SSO, and RBAC contributes significantly to maintaining data confidentiality, integrity, and availability, while still considering the needs and context of each organization.*

Keyword: *Multi-Factor Authentication (MFA), Single Sign-On (SSO), Role-Based Access Control (RBAC), Information Security Systems.*

Abstrak: Penelitian ini membahas efektivitas Multi-Factor Authentication (MFA), Single Sign-On (SSO), dan Role-Based Access Control (RBAC) sebagai mekanisme utama untuk meningkatkan keamanan sistem informasi. Melalui studi literatur yang bersumber dari jurnal, buku, dan prosiding, penelitian ini menilai kemampuan ketiga metode tersebut dalam melindungi data dan mencegah akses tidak sah. Hasil kajian menunjukkan bahwa MFA menambah lapisan verifikasi yang mampu menurunkan risiko pembobolan akun, SSO meningkatkan efisiensi autentikasi dengan satu kali login untuk berbagai layanan, dan RBAC mengatur hak akses secara terstruktur berdasarkan peran pengguna. Integrasi ketiganya terbukti dapat membangun arsitektur keamanan yang lebih kuat dan adaptif. Penelitian ini menegaskan bahwa penerapan MFA, SSO, dan RBAC berkontribusi signifikan dalam menjaga kerahasiaan, integritas, dan ketersediaan data, dengan tetap mempertimbangkan kebutuhan dan konteks tiap organisasi.

Kata Kunci: Multi-Factor Authentication (MFA), Single Sign-On (SSO), Role-Based Access Control (RBAC), Keamanan Sistem Informasi.

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah mendorong organisasi untuk memanfaatkan sistem digital dalam pengelolaan data dan operasional sehari-hari. Namun, meningkatnya digitalisasi juga diikuti oleh berbagai ancaman keamanan, seperti pencurian identitas, akses ilegal, dan manipulasi data. Kondisi ini menuntut organisasi untuk memiliki sistem keamanan informasi yang memadai agar risiko penyalahgunaan data dapat diminimalkan. Keamanan Sistem Informasi merujuk pada upaya yang dilakukan untuk menghentikan penipuan atau paling tidak mengidentifikasi adanya tindakan curang dalam suatu sitem yang didasarkan pada informasi di mana informasi tersebut tidak memiliki makna fisik (G. J. Simons, 2018). Salah satu aspek terpenting dalam keamanan sistem informasi adalah otentikasi dan kontrol akses. Password adalah metode otentikasi yang banyak digunakan dalam beberapa sistem keamanan (Sudiarto Raharjo et al., 2017). Namun, penggunaan kata sandi sebagai metode tradisional semakin dianggap tidak memadai. Alat pemecah kata sandi modern seperti *John the Ripper* dan *Hashcat* telah mengintegrasikan pendekatan probabilistik, termasuk *Markov Chains* dan *Probabilistic Context-Free Grammars* (PCFG), sehingga mampu menebak kata sandi buatan manusia dengan jauh lebih efisien. Penelitian klasik oleh Bonneau menunjukkan bahwa pengguna cenderung memilih kata sandi yang sangat mudah diprediksi, sehingga meningkatkan kerentanan terhadap serangan berbasis probabilistic. Dalam mengatasi berbagai metode serangan kontemporer seperti phishing, serangan brute force, dan pengisian kredensial, sistem autentikasi yang bergantung pada password sepertinya sudah tidak cukup. Ini mengindikasikan bahwa diperlukan upaya pengamanan tambahan.

Tiga mekanisme yang kini menjadi standar dalam keamanan modern adalah MFA, SSO, dan RBAC. Menurut Khan et al. (2023) MFA berperan penting dalam meningkatkan keamanan karena menggabungkan beberapa metode verifikasi. Tidak seperti autentikasi tradisional yang hanya mengandalkan kata sandi, MFA mengintegrasikan berbagai elemen, seperti biometrik (sidik jari, pengenalan wajah), token keamanan, atau kode OTP (One-Time Password) (Andriotis et al., 2023). Sementara itu, Single Sign On merupakan sebuah sistem yang memungkinkan pengguna untuk hanya perlu mengingat satu nama pengguna dan kata sandi yang sah untuk mengakses berbagai layanan secara bersamaan (Priyo Puji Nugroho, 2012:21). SSO menghentikan kebutuhan login yang berulang dengan mengenali individu secara tepat dan memungkinkan pemakaian kembali data autentikasi pada sistem yang dapat diandalkan. Pendekatan ini meningkatkan kenyamanan pengguna serta menurunkan kemungkinan bahaya yang disebabkan oleh pemakaian kata sandi yang kurang kuat atau pengelolaan informasi akses yang tidak terkendali. Di sisi lain, RBAC merupakan mekanisme yang mengelola berbagai hak akses dengan tingkat fleksibilitas yang lebih tinggi jika dibandingkan dengan model kontrol akses Kontrol Akses Wajib (MAC) maupun Kontrol Akses Discretionary (DAC) (Habib, 2011).

Penelitian - penelitian terdahulu menunjukkan keberhasilan penerapan ketiga mekanisme tersebut. Misalnya, studi oleh Badeges & Fauzi (2023) menunjukkan bahwa penerapan MFA pada phpMyAdmin secara efektif meningkatkan keamanan akses database. Penelitian lain oleh Wibowo et.al (2013) menunjukkan bahwa implementasi sistem SSO terintegrasi antara captive portal, aplikasi STIKOM, dan Google Apps berhasil mengurangi waktu login, meningkatkan efisiensi, dan memperbaiki keamanan sistem. Sementara itu, studi Khairi & Alda (2024) menunjukkan bahwa penerapan RBAC dapat meningkatkan keamanan dan privasi data anggota koperasi dengan membatasi hak akses pengguna sesuai perannya.

Temuan dari berbagai penelitian tersebut menunjukkan bahwa MFA, SSO, dan RBAC memiliki peran strategis dalam memperkuat keamanan sistem informasi. Namun, setiap mekanisme tentu memiliki kelebihan, tantangan, dan konteks penerapan yang berbeda. Oleh

karena itu, perlu dilakukan kajian lebih mendalam melalui studi literatur untuk memahami bagaimana ketiga mekanisme ini bekerja, seberapa efektifnya, serta apa saja kekurangannya jika diterapkan pada organisasi yang berbeda.

Berdasarkan latar belakang tersebut, maka dapat dirumuskan beberapa permasalahan yang akan dibahas dalam penelitian ini, yaitu:

1) Bagaimana penerapan Multi-Factor Authentication (MFA), Single Sign-On (SSO), dan Role-Based Access Control (RBAC) dalam keamanan sistem informasi?
2) Seberapa efektif MFA, SSO, dan RBAC dalam meningkatkan perlindungan data dan mencegah akses tidak sah?
3) Bagaimana hasil penelitian sebelumnya menggambarkan penggunaan MFA, SSO, dan RBAC dalam meningkatkan keamanan sistem informasi?

METODE

Metode dalam penelitian ini menggunakan metode studi pustaka dengan pendekatan literature review untuk mengetahui bagaimana multi-factor authentication, single sign-on, dan role-based acces control diterapkan dalam sistem informasi. Creswell (2016) mengungkapkan bahwa literature review adalah sebuah metodologi penelitian yang dimaksudkan untuk mengumpulkan dan menarik intisari dari penelitian sebelumnya dengan menganalisis beberapa overview para ahli yang tertera dalam teks. Pendekatan sesuai dengan literature review memungkinkan penulis atau peneliti dapat mengambil banyak penelitian yang sudah ada yang sudah tidak relevan dengan topik keamanan tersebut. Secara studi pemanfaatan berbagai sumber ilmiah antara lain jurnal nasional dan internasional, buku, dan proceiding individual topik keamanan akses. Sumber-sumber yang sesuai kemudian dibaca dan di analisis dengan cara mengindentifikasi tema atau ide utama yang berkaitan dengan MFA, SSO, dan RBAC. Melalui metode ini, penelitian dapat menyajikan penjelasan yang runtut dan menyeluruh tanpa harus melakukan pengumpulan data lapangan, namun tetap memenuhi kaidah akademik.

HASIL DAN PEMBAHASAN

Berdasarkan latar belakang masalah dan rumusan masalah diatas, maka hasil penelitian ini adalah sebagai berikut:

Multi-Factor Authentication (MFA)

Autentikasi, juga dikenal sebagai proses verifikasi identitas agar dapat dimasukkan ke dalam suatu sistem (Saputra , 2021) .sebuah identitas agar dapat dimasukkan ke dalam suatu sistem (Saputra, 2021). Proses ini sangat penting dalam menjaga keamanan karena memastikan bahwa hanya individu yang berhak masuk ke sistem. Secara umum, otentikasi dilakukan melalui tiga faktor yang umum dijumpai, yaitu “something you know”, “something you have”, dan “something you are”. Ketiga faktor tersebut mencakup kata sandi atau PIN, perangkat fisik seperti token atau kartu pintar, serta karakteristik biometrik seperti sidik jari dan pengenalan wajah.

Autentikasi tunggal dinilai semakin lemah karena mudah ditembus oleh pihak yang tidak berhak. Dengan hanya mengandalkan username dan password, risiko kebocoran atau pencurian kredensial sangat besar. Oleh karena itu, diperlukan faktor verifikasi tambahan seperti kode OTP atau sidik jari. Kebutuhan inilah yang melahirkan metode keamanan yang lebih kuat, yaitu MFA.

MFA adalah sistem keamanan yang menggunakan lebih dari satu cara yang terpisah untuk memastikan identitaspengguna agar dapat memverifikasi identitasnya sehingga mereka dapat melanjutkan atau menyelesasikan transaksi lainnya. Sistem ini memastikan bahwa pengguna benar-benar pihak yang berwenang dengan mengkombinasikan dua atau lebih metode verifikasi dari faktor yang berbeda. Menurut Khan et al. (2023), pentingnya otentikasi multi-faktor yaitu dapat meningkatkan keamanan dengan menggabungkan beberapa metode verifikasi Ini sejalan dengan temuan yang diperoleh oleh Andriotis ed al. (2023) yang menjelaskan bahwa penggunaan biometrik dan OTP membuat serangan berbasis pencurian

kredensial menjadi jauh lebih sulit. Apabila salah satu metode verifikasi gagal bahkan bocor, data pengguna tetap aman karena peretas tetap membutuhkan metode verifikasi lainnya untuk bisa mengakses sistem.

Saat ini, MFA telah banyak digunakan pada beberapa platform digital seperti layanan keuangan, surtel, jaringan sosial, dan aplikasi korporat.Misalnya, ketika pengguna mengaktifkan MFA pada platform media sosial seperti Facebook, mereka diwajibkan memasukkan verifikasi tambahan berupa kode OTP atau melalui aplikasi autentikator sebelum dapat melakukan login. Mekanisme ini terbukti efektif untuk mencegah pembobolan akun akibat kebocoran kata sandi.

Penerapan Single Sign-On (SSO)

Sign-On adalah sistem dimana pengguna hanya perlu melakukan satu kali proses login ke layanan atau aplikasi. Menurut Fauziah (2014) bahwa penerapan Single Sign On atau SSO merupakan suatu cara agar pengguna dapat diakses beberapa layanan tertentu yang ada dalam satu jaringan dengan melakukan autentikasi sekali saja. Dengan mekanisme ini, pengguna tidak perlu melakukan login berulang-ulang meskipun berpindah ke platform lain. Saat menggunakan SSO, ini dapat ditingkatkan efisien jaringan secara keseluruhan sambil mengontrol parameter sistem yang relevan.

SSO juga punya beberapa kelebihan. Salah satunya, pengguna jadi lebih mudah mengakses layanan tanpa harus mengingat banyak username dan password. Contohnya pada sistem layanan perpustakaan, SSO memungkinkan pengguna login sekali dan memperoleh akses ke seluruh layanan yang terintegrasi tanpa perlu melakukan autentikasi ulang. Selain memberikan kenyamanan bagi pengguna, SSO juga memudahkan administrator dalam memberikan izin akses dan memantau aktivitas pengguna karena semuanya bisa dilihat dari satu tempat.

Selain itu, penerapan sistem Single Sign-On (SSO) yang mengintegrasikan autentikasi login dari beberapa aplikasi serta penyimpanan data pengguna pusat, mampu mengurangi beban server. Misalnya, ketika pengguna login di satu aplikasi, aplikasi lain akan otomatis ikut terbuka. Begitu juga ketika pengguna log out, semua aplikasi akan keluar secara bersamaan. Ini membuat proses login dan log out jadi lebih efisien dan aman.

Pada beberapa organisasi besar, SSO biasanya bekerja dengan sistem bernama Central Authentication Service (CAS), yang membantu mengatur proses login supaya tetap cepat dan stabil Dengan cara ini, nilai-nilai yang mencerminkan efektivitas SSO dalam mengelola otentikasi pengguna dapat dicapai. Dalam berbagai bidang, khususnya pendidikan dan perusahaan besar, penerapan SSO terbukti telah meningkatkan efisien. Penerapan skema SSO yang mengambil alih proses autentikasi membuat proses autentikasi hanya dilaksanakan sekali. Dengan demikian, SSO mampu menciptakan pengalaman digital yang lebih praktis sekaligus meningkatkan kinerja organisasi dalam mengelola sumber daya digital.

Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) adalah sebuah mekanisme pengelolaan sejumlah hak akses yamg lebih fleksibel dibandingkan dengan model kontrol akses Mandatory Access Control (MAC) maupun Discretionary Access Control (DAC) (Habib, 2011). Dengan model ini, setiap pengguna hanya dapat menerapkan tindakan yang sesuai dengan perannya, sehingga akses terhadap data dan sumber daya menjadi lebih terkontrol. RBAC adalah model keamanan yang mengatur hak akses berdasarkan peran yang telah ditentukan sebelumnya, sehingga setiap pengguna hanya dapat melakukan aktivitas sesuai otoritas jabatannya (Sandhu et al, 1996).

RBAC adalah salah satu metode kontrol akses digunakan untuk mengontrol akses pengguna dalam suatu sistem dengan peran atau jabatannya di dalam suatu organisasi. Dengan cara ini, organisasi dapat lebih mudah menyesuaikan hak akses berdasarkan tugas dan tanggung jawab setiap pengguna tanpa harus mengatur izin satu per-satu.

Pada sistem RBAC terdapat tiga komponen utama, yaitu pengguna (users), peran (roles), dan izin (permissions). Pengguna adalah individu yang mengakses sistem, peran menggambarkan posisi atau tanggung jawab tertentu dalam organisasi, dan izin adalah hak yang menentukan apa saja yang bisa dilakukan terhadap suatu data atau sumber daya. Mekanisme ini membuat pengelolaan akses menjadi lebih efisien karena administrator hanya perlu mengatur izin pada level peran, bukan pada setiap pengguna

RBAC banyak digunakan dalam organisasi modern karena dapat meningkatkan keamanan data dan mencegah akses ilegal. Dengan membatasi tindakan pengguna berdasarkan perannya, risiko penyalahgunaan data dapat ditekan. Selain itu, RBAC mempermudah proses audit dan pemantauan aktivitas pengguna karena setiap peran sudah memiliki batasan akses yang jelas. Model ini sangat bermanfaat terutama bagi organisasi berskala besar yang memiliki struktur kerja kompleks dan banyak pengguna.

Hasil Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu

No	Author	Judul Penelitian	Hasil Penelitian	Perbedaan	Persamaan
1	Komang Gede Jaya Wira Buana, Lilik Widyawati, dan Ondi Asroni	Analisis Dan Implementasi Keamanan Authentication Menggunakan Multi Factor Authentication (MFA) pada Aplikasi Web.	Hasil penelitian membuktikan bahwa penerapan Multi-Factor Authentication (MFA) dengan Google Authenticator dan verifikasi email mampu meningkatkan keamanan autentikasi secara signifikan. keamanan pada sistem login modern.	Perbedaannya terletak pada fokus penelitiannya. Dimana jurnal ini lebih mendalam dalam analisis dan implementasi MFA spesifik dengan Google Authenticator dan verifikasi. Sedangkan jurnal penulis berfokus pada penyajian pengamatan yang lebih komprehensif tentang beberapa mekanisme keamanan (MFA, SSO, RBAC) dan sinerginya.	Keduanya sama-sama melakukan peningkatan keamanan sistem informasi melalui penggunaan Multi-Factor Authentication (MFA).
2	Hpaeruddin, Stefanus Eko Prasetyo, dan Avista Mindy	Implementasi Multi-Factor Authentication Untuk Optimalisasi Keamanan Akses Data	Hasil penelitian membuktikan bahwa penerapan Multi-Factor Authentication (MFA) menggunakan Auth0 pada sistem WordPress PT. ABC mampu meningkatkan keamanan akses data secara signifikan.	Perbedaan nya terletak pada fokus penelitiannya. Jurnal ini lebih membahas pada implementasi langsung MFA pada PT. ABC dan terbukti meningkatkan keamanan melalui pengujian teknis. Sedangkan jurnal penulis hanya menjelaskan konsep MFA, SSO, dan RBAC secara umum tanpa penerapan nyata, sehingga hasilnya bersifat teoritis, bukan praktik lapangan.	Keduanya sama-sama menekankan pentingnya peningkatan keamanan sistem informasi, khususnya melalui penggunaan Multi-Factor Authentication (MFA).

3	M Zidane Al-Ghifary	PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN MULTI-FAKTOR BERBASIS PENGENALAN WAJAH UNTUK APLIKASI MOBILE BANKING.	Hasil penelitian menunjukkan bahwa sistem keamanan multi-faktor berbasis pengenalan wajah yang dikembangkan mampu meningkatkan perlindungan pada aplikasi mobile banking secara signifikan. Teknologi pengenalan wajah yang digunakan berhasil memverifikasi identitas pengguna dengan akurat, terutama ketika digabungkan dengan faktor keamanan tambahan seperti kata sandi dan sidik jari.	Perbedaannya terletak pada fokus dan cakupan penerapannya. Jurnal ini menitikberatkan pada penerapan MFA berbasis pengenalan wajah khusus untuk mobile banking. Sedangkan jurnal penulis membahas arsitektur keamanan yang lebih luas dengan menggabungkan MFA, SSO, dan RBAC untuk berbagai jenis sistem informasi, bukan hanya satu domain tertentu.	Keduanya sama-sama menekankan pentingnya verifikasi ganda untuk mencegah akses tidak sah dan melindungi data pengguna.
4	Muhammad Iftikhar Hussain, Jingsha Dia, Nafei Zhu, Fahad Sabah, Zulfikar Ali Zardari, Saqib Hussain, dan Fahad Razque	AAAA: Implementasi SSO dan MFA di Multi-Cloud untuk Mitigasi Meningkatnya Ancaman dan Kekhawatiran Terkait Metadata Pengguna	Penelitian ini menunjukkan bahwa penggabungan MFA dan SSO secara efektif memperkuat keamanan di lingkungan multi-cloud. Kerangka keamanan yang dirancang mampu mencegah lebih dari 93% bahaya siber, termasuk brute-force, man-in-the-middle, dan rekayasa sosial. Hasilnya, MFA terbukti lebih	Perbedaannya terletak pada empat aspek utama, yaitu lingkup, mekanisme tambahan, jenis ancaman, dan penekanan hasil. Jurnal ini meneliti implementasi SSO dan MFA dalam lingkungan multi-cloud, sehingga pembahasannya lebih kompleks dengan penekanan pada Federated Trust dan evaluasi keamanan melalui AAAA, serta mencakup berbagai ancaman siber tingkat lanjut.	Keduanya mempunyai persamaan yaitu sama-sama memakai MFA untuk menambah lapisan keamanan saat login, dan SSO untuk mempermudah pengguna agar tidak perlu berulang kali memasukkan akun.

			unggul dari SSO dalam menjaga akuntabilitas dan ketersediaan sistem.		
5	Walid Badeges dan Muhammad Naufal Fauzi	IMPLEMENTASI MULTI FACTOR AUTHENTICATION PADA PHPMYADMIN	Hasil penelitian ini menunjukkan bahwa penerapan Multi-Factor Authentication (MFA) pada phpMyAdmin secara efektif mengembangkan keamanan akses database. Integrasi Google Authenticator mampu menambahkan lapisan verifikasi tambahan sehingga akses tidak sah dapat dicegah meskipun password utama bocor.	Perbedaan kedua jurnal tersebut terlihat dari fokus dan cakupan keamanan yang dibahas. Jurnal ini hanya menitikberatkan pada penerapan MFA berbasis Google Authenticator untuk memperkuat autentikasi akses database, sehingga ruang lingkupnya lebih sempit dan teknis. Sebaliknya, jurnal penulis membahas keamanan sistem informasi secara lebih luas karena tidak hanya mengimplementasikan MFA, tetapi juga SSO dan RBAC sebagai tiga lapisan keamanan yang saling melengkapi	Keduanya sama-sama menekankan pentingnya Multi-Factor Authentication (MFA) sebagai mekanisme utama untuk memperkuat proses autentikasi dan melindungi akses ke sistem atau data sensitif. Baik pada implementasi di phpMyAdmin maupun pada sistem yang lebih luas, kedua penelitian ini bertujuan mengurangi risiko kebocoran, penyalahgunaan akses, serta memperkuat perlindungan terhadap ancaman siber.

Berdasarkan hasil penelitian diatas, maka pembahasan artikel ini yaitu dengandilakukan review terhadap penelitian terdahulu yang relevan, analisis pengaruh antar variabel serta membuat kerangka konseptual penelitian.

Implementasi Multi-Factor Authentication dalam Keamanan Sistem Informasi

Salah satu strategi utama dalam meningkatkan keamanan sistem informasi adalah penerapan Multi-Factor Authentication (MFA). Beberapa sistem keamanan modern telah berbasis hash sebagai lapisan perlindungan tambahan (Stallings, 2018). Bagi pengguna, sangat disarankan untuk selalu menggunakan password yang panjang, kompleks, dan unik untuk setiap akun yang dimiliki. Selain itu, aktivasi autentikasi MFA dapat memberikan lapisan keamanan tambahan dalam proses login.

MFA merupakan metode keamanan penting yang menggabungkan dua atau lebih faktor autentikasi, di mana penggunaan MFA memiliki potensi besar untuk menurunkan kemungkinan terjadinya pencurian identitas dan penipuan (Aziza et al., 2025). Strategi keamanan ini menjadi

elemen dari pendekatan komprehensif untuk mengatasi bahaya siber, yang mencakup penegakan peraturan keamanan yang ketat, penerapan teknologi terbaru, serta pelatihan pemahaman keamanan untuk semua pengguna sistem (Saputra et al., 2023). Signifikansi verifikasi identitas pengguna ada pada kemampuannya untuk menghindari masuknya pihak yang tidak berwenang ke dalam informasi sensitif, karena pengaturan akses mencakup pengelolaan hak akses pada data, sistem, atausumber daya tertentu dengan tujuan memelihara kerahasiaan, integritas, dan ketersediaan data (Wahyudi et al., 2020).

Autentikasi Multi-Faktor menggabungkan dua atau lebih faktor, seperti informasi yang dikenal oleh pengguna (password), dimiliki oleh pengguna (kode OTP atau token yang berubah-ubah), atau sifat biometrik pengguna (pengenalan wajah atau sidik jari). Penerapan MFA secara signifikan mengurangi risiko pencurian identitas, penipuan, dan akses ilegal ke data sensitif. Di samping itu, MFA dapat dikombinasikan dengan mekanisme lain seperti SSO, atau RBAC untuk membentuk lapisan keamanan yang lebih komprehensif, terutama pada sistem berskala besar atau layanan berbasis cloud. Di sisi lain, metode peretasan dalam sistem keamanan data melibatkan serangkaian cara yang diterapkan oleh peretas untuk mendapatkan akses ilegal ke informasi atau sistem yang telah dilindungi (Rasaputhra et al., 2024).

Meskipun efektif, implementasi MFA juga menghadapi tantangan, termasuk penggunaan password yang kurang kuat atau identik di berbagai akun yang bisa mengurangi tingkat keamanannya. Oleh karena itu, faktor autentikasi yang tepat dan penerapan kebijakan kata sandi yang aman sangat penting (Ometov et al., 2018). Secara keseluruhan, MFA memberikan perlindungan berlapis yang efektif, meningkatkan keamanan teknis, sekaligus membangun kepercayaan pengguna terhadap sistem. Implementasi ini kini dianggap sebagai praktik standar dalam mengamankan sistem informasi modern, dan penerapannya direkomendasikan untuk berbagai jenis aplikasi, mulai dari web, perusahaan, sampai layanan mobile banking (Badeges & Fauzi, 2023). Pembahasan mengenai penerapan MFA ini juga sejalan dengan beberapa penelitian sebelumnya seperti (Buana et al., 2025), (Haeruddin et al., 2025), (Hussain et al., 2021), dan (Bedeges et al., 2023), yang menyoroti pentingnya autentikasi berlapis dalam meningkatkan ketahanan sistem dari ancaman siber.

Implementasi Single Sign-On dalam Keamanan Sistem Informasi

Penerapan SSO semakin dipandang sebagai pendekatan strategis untuk memperkuat keamanan sekaligus menyederhanakan proses autentikasi pada berbagai layanan digital. Dengan mekanisme masuk sekali untuk banyak sistem, pengguna tidak lagi terbebani oleh keharusan mengingat beberapa kombinasi username dan kata sandi. Pada saat yang sama, organisasi dapat mengelola identitas pengguna melalui satu pusat kontrol, sehingga proses administrasi menjadi lebih efisien. Konsep Single Sign-On (SSO) berbasis LDAP ternyata dapat mengatasi masalah konsep sebelumnya karena pengguna hanya perlu mengautentikasi sekali untuk mendapatkan hak akses ke semua layanan dalam jaringan (Futuh Hilmi, Mangkudjaja & Irawan, 2020). Dalam praktiknya, integrasi ini menciptakan pengalaman akses yang jauh lebih cepat dan konsisten.

Dari perspektif operasional, SSO menawarkan kontribusi besar terhadap efisiensi kerja. Alur masuk ke sejumlah aplikasi menjadi lebih ringkas dan seragam, sehingga pengguna tidak perlu mengulang proses autentikasi setiap kali berpindah layanan. Selain memberikan kenyamanan, pendekatan ini berdampak pada peningkatan keamanan karena meminimalkan kecenderungan pengguna memakai kata sandi yang sama di berbagai platform. Dengan sistem autentikasi yang terpusat, organisasi dapat menerapkan standar keamanan yang lebih ketat dan konsisten pada seluruh aplikasi yang berada dalam ekosistemnya.

\Sejumlah penelitian lain yang menyoroti penggunaan SSO berbasis direktori pusat turut menegaskan bahwa konsolidasi kredensial mampu memperkuat kontrol akses, mempermudah proses penerbitan dan penonaktifan akun, serta menekan potensi penyalahgunaan identitas (Ruswandi & Alijoyo, 2024). Meski demikian, implementasi SSO bukan tanpa risiko. Tantangan seperti potensi single point of failure serta kerentanan konfigurasi perlu mendapat perhatian

khusus. Untuk itu, mekanisme perlindungan tambahan misalnya enkripsi token, pembaruan sesi secara berkala, dan penggunaan autentikasi multi-faktor diperlukan guna memastikan sistem tetap aman meskipun berada dalam skenario ancaman yang dinamis (Arianto, Witanti & Ashaury, 2025).

Implementasi Role-Based Acces Control dalam Keamanan Sistem Informasi

Penerapan RBAC kini telah menjadi salah satu pendekatan utama dalam pengelolaan keamanan sistem informasi yang modern. Mekanisme ini mengatur hak akses berdasarkan peran yang dimiliki pengguna, bukan berdasarkan identitas pengguna secara individual, sehingga kontrol akses menjadi lebih konsisten dan mudah dikelola (Prasetia & Manongga, 2024). Berbagai studi menunjukkan bahwa RBAC mampu meningkatkan akurasi konfigurasi izin, mengurangi potensi kesalahan administrasi, serta mempercepat proses pengelolaan hak akses di lingkungan organisasi.

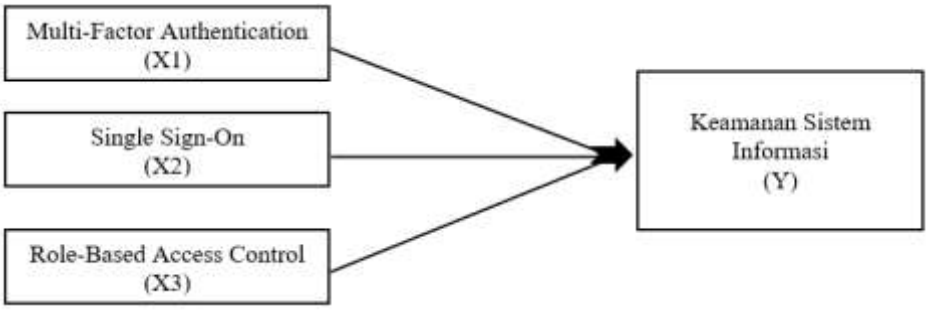
Dalam konteks aplikasi web, RBAC memungkinkan penerapan pemisahan tugas (segregation of duties) melalui pengaturan izin berbasis peran seperti admin, staff, maupun viewer. Hasil penelitian menegaskan bahwa implementasi tersebut dapat meningkatkan keamanan karena setiap tindakan pengguna selalu diverifikasi melalui permission yang terikat pada perannya. Dengan demikian, peluang terjadinya akses ilegal dapat diminimalkan (Arifin & Rahmah, 2023). RBAC menjadikan alur pemberian izin lebih sistematis, terutama pada sistem yang memiliki jumlah pengguna besar dan kebutuhan akses kompleks.

Selain itu, penelitian literatur terbaru menegaskan bahwa RBAC mendukung penerapan prinsip least privilege, yakni pemberian akses hanya sesuai kebutuhan pengguna. Prinsip ini berperan penting dalam menjaga integritas dan kerahasiaan data, sekaligus memperkuat penerapan kebijakan keamanan berlapis pada sistem informasi modern (Hernawan et al., 2024). Dengan tidak perlu memberikan izin secara manual pada setiap pengguna, administrator cukup mengelola akses pada level peran, sehingga beban administrasi menjadi jauh lebih ringan dan efisien (Pratama & Wicaksono, 2022).

Berdasarkan berbagai temuan tersebut, dapat disimpulkan bahwa RBAC merupakan komponen esensial dalam arsitektur keamanan sistem informasi, terutama pada sistem berskala besar dan multi-user. RBAC menyediakan mekanisme pengelolaan izin yang lebih terstruktur, aman, dan mudah dipelihara, tanpa memerlukan konfigurasi ulang secara individual pada setiap pengguna.

Kerangka Konseptual

Bedasarkan rumusan masalah, analisis, dan kajian sebelumnya yang terkait serta inti dari pembahasan mengenai dampak antar variabel. Dengan demikian, disusunlah kerangka konsep berikut ini:



Gambar 1. Kerangka Konseptual

Bedasarkan gambar 1 kerangka konseptual diatas, maka diperoleh:

1. H1: Multi-factor Authentication (X^1) berpengaruh terhadap Keamanan Sistem Informasi (Y).
2. H2: Single Sign-On (X^2) berpengaruh terhadap Keamanan Sistem Informasi (Y).

3. H3: Role-Based Acces Control (X^3) berpengaruh terhadap Keamanan Sistem Informasi (Y).

KESIMPULAN

Berdasarkan hasil kajian literatur, dapat disimpulkan bahwa penerapan MFA, SSO, dan RBAC merupakan strategi yang efektif dalam memperkuat keamanan sistem informasi modern. MFA memberikan lapisan verifikasi tambahan yang mampu mengurangi risiko pencurian identitas dan akses tidak sah, sehingga memperkuat kemampuan sistem untuk menghadapi berbagai jenis ancaman dunia maya. SSO memberikan kemudahan dan efisiensi dalam proses autentikasi dengan membuat pengguna untuk mengakses beberapa layanan melalui satu kali masuk, sekaligus mempermudah pengelolaan identitas secara terpusat. Sementara itu, RBAC terbukti mampu meningkatkan kontrol akses dengan menetapkan hak dan izin berdasarkan peran pengguna, sehingga mendukung prinsip least privilege dan mengurangi kompleksitas administrasi. Ketiga mekanisme tersebut, ketika diintegrasikan, dapat menghasilkan arsitektur keamanan yang lebih komprehensif, adaptif, dan andal bagi organisasi berskala besar maupun sistem multi-user. Oleh karena itu, kombinasi MFA, SSO, dan RBAC direkomendasikan sebagai pendekatan utama dalam usaha untuk melindungi privasi, keutuhan, dan aksebilitas data dalam sistem informasi.

REFERENSI

Akuthota, A. K. (2025). Role-based access control (RBAC) in modern cloud security governance: An in-depth analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 45-52.

Alaca, F., & Oorschot, P. C. V. (2020). Comparative analysis and framework evaluating web single sign-on systems. ACM Computing Surveys (CSUR), 53(5), 1-34. https://dl.acm.org/doi/abs/10.1145/3409452

Al-Ghifary, MZ PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN MULTI-FAKTOR BERBASIS PENGENALAN WAJAH UNTUK APLIKASI MOBILE BANKING.

Alijoyo, F. A. (2024). PENGEMBANGAN SINGLE SIGN ON (SSO) MENGGUNAKAN TEKNOLOGI MAGIC LINK DI UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMMI). Jurnal Informatika dan Rekayasa Elektronik, 7(1), 115-123. http://e-journal.stmiklombok.ac.id/index.php/jire

Akuthota, A. K. (2025). Role-based access control (RBAC) in modern cloud security governance: An in-depth analysis. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(2), 45-52.

Andriotis, P., Kirby, M., & Takasu, A. (2023). Bu-Dash: a universal and dynamic graphical password scheme (extended version). International Journal of Information Security, 22(2), 381–401. https://doi.org/10.1007/s10207-022-00642-2

Andriotis, P., Kirby, M., & Takasu, A. (2023). Bu-Dash: a universal and dynamic graphical password scheme (extended version). International Journal of Information Security, 22(2), 381–401. https://doi.org/10.1007/s10207-022-00642-2

Arianto, I. G., Witanti, W., & Ashaury, H. (2025). Sistem Keamanan Otentikasi Pengguna Pada Modul Single Sign On Menggunakan OAuth 2.0 dan One Time Password. Jurnal Ilmu Komputer dan Teknologi, 6(1), 25-31. https://ejournal.uhb.ac.id/index.php/IKOMTI/article/view/1768

Arifin, Z., & Rahmah, D. (2023). *Implementasi Role-Based Access Control (RBAC) pada Sistem Informasi Berbasis Web untuk Peningkatan Keamanan Akses*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 7(3), 1123–1131.

Armanda, A. S., Shaleha, I., & Fatwanto, A. RANCANGAN FITUR SINGLE SIGN ON PADA PADA PERPUSTAKAAN XYZ. Jurnal Informasi, Perpustakaan, dan Kearsipan (JIPKA), 3(1), 14-26. https://doi.org/10.26418/jipka.v3i1.71614

Aziza, N., & Wardhani, D. F. (2025). Evaluasi Keamanan Aplikasi Mobile Banking: Ancaman, Perlindungan dan Studi Kasus Pada Sistem Perbankan Digital. Jurnal Ilmiah Teknologi Informasi dan Robotika, 7(1), 11-22.

Badeges, W., & Fauzi, M. N. (2023). Implementasi multi factor authentication pada phpMyAdmin. TRIPLE A: Jurnal Pendidikan Teknologi Informasi, 2(1), 35–39.

Bonneau, J. (2012, May). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE symposium on security and privacy* (pp. 538-552). IEEE. https://ojs.unikom.ac.id/index.php/jamika

Buana, K. G. J. W., Widyawati, L., & Asroni, O. (2025). Analisis dan Implementasi Keamanan Authentication Menggunakan Multi Factor Authentication (MFA) Pada Aplikasi Web. CORISINDO 2025, 1, 501-510.

Cahyanto, I., Madihah, H., Budiarso, I., Sutrisno, A., & Hidayat, T. (2024). Effectiveness Of Multifactor Authentication Technology For Protecting Student Privacy: A Systematic Literature Review. Edum Journal, 7(2), 253-269. https://doi.org/10.31943/edumjournal.v7i2.286

Creswell, J, W. (2016). Research design: pendekatan metode, kuantitatif, dan campuran (4), Yogyakarta: Pustaka Pelajar.

Gemawaty, C. A., & Yuliani, Y. (2024). MANAJEMEN IDENTITAS DAN AKSES DALAM KEAMANAN SISTEM INFORMASI (PENDEKATAN LITERATURE REVIEW). Jurnal Manajamen Informatika Jayakarta, 4(4), 396-403. https://doi.org/10.52362/jmijayakarta.v4i4.1527

Habib, M. A. 2011. Role inheritance with object-based DSD. International Journal Internet Technology and Secured Transactions 3(2):149–60

Haeruddin, H., Prasetyo, S. E., & Mindy, A. (2025). Implementasi Multi-Factor Authentication Untuk Optimalisasi Keamanan Akses Data Di PT. ABC. Jurnal Manajemen Informatika (JAMIKA), 15(1), 85096-85096. doi: https://ojs.unikom.ac.id/index.php/jamika

Hafizd, K. A. (2021). PERANCANGAN SINGLE SIGN ON (SSO) PADA APLIKASI WEB MENGGUNAKAN CLOUD IDENTITY:(STUDI KASUS: POLITEKNIK NEGERI TANAH LAUT). Antivirus: Jurnal Ilmiah Teknik Informatika, 15(2), 242-251. https://doi.org/10.35457/antivirus.v15i2.1813

Hilmi, F., Mangkudjaja, R., & Irawan, B. (2012). Analisis Performansi Autentikasi Single Sign On pada Web Menggunakan LDAP. Jurnal SIFO Mikroskil, 13(2), 93-102. https://ejurnal.mikroskil.ac.id/index.php/jsm/article/view/74

Hernawan, R., Nugroho, S., & Latif, A. (2024). *RBAC dan Penerapan Prinsip Least Privilege dalam Sistem Informasi Modern*. International Journal of Computer Theory and Engineering, 16(1), 45–52.

Hussain, M. I., He, J., Zhu, N., Sabah, F., Zardari, Z. A., Hussain, S., & Razque, F. (2021). AAAA: SSO and MFA implementation in multi-cloud to mitigate rising threats and concerns related to user metadata. Applied Sciences, 11(7), 3012. https://doi.org/10.3390/app11073012

J. Williamson and K. Curran, “The Role of Multi-factor Authentication for Modern Day Security,” Semicond. Sci. Inf. Devices, vol. 3, no. 1, pp. 16–23, 2021, doi: 10.30564/ssid.v3i1.3152.

Khairi, A. S. (2024). Implementasi Role Based Access Control dalam Pengelolaan Hak Akses Koperasi Berbasis Mobile. Jurnal Teknik Informatika Unika ST. Thomas (JTIUST), 9(1).

Khan, M. A., Alhakami, H., Alhakami, W., Shvetsov, A. V., & Ullah, I. (2023). A Smart Card-Based Two-Factor Mutual Authentication Scheme for Efficient Deployment of an IoT-Based Telecare Medical Information System. Sensors, 23(12). **https://doi.org/10.3390/s23125419**

Khan, M. A., Alhakami, H., Alhakami, W., Shvetsov, A. V., & Ullah, I. (2023). A Smart Card-Based Two-Factor Mutual Authentication Scheme for Efficient Deployment of an IoT-Based Telecare Medical Information System. Sensors, 23(12). https://doi.org/10.3390/s23125419

M. E. Shacklett and T. Contributor, “Multifactor Authentication (MFA),” 2021. https://searchsecurity.techtarget.com/definiti on/multifactor-authentication-MFA. (accessed May. 18, 2021). https://www.neliti.com/publications/497955/library-self-service-system-using-nfc-and-2fa-google-authenticator

M. Stamp, “Information Security: Principles and Practices” San Jose, CA: Wiley, 2011, hal 276.

Mashudi, A. I. A., & Prihanto, A. (2025). Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication. Journal of Informatics and Computer Science (JINACS), 6(03), 630-638.https://doi.org/10.26740/jinacs.v6n03.p630-638

Mukhlisin, M., & Firmansyah, R. A. (2025). ZERO TRUST ARCHITECTURE: SOLUSI KEAMANAN DAN PRIVASI UNTUK INSTITUSI PENDIDIKAN, SYSTEMATIC LITERATURE REVIEW. JATI (Jurnal Mahasiswa Teknik Informatika), 9(4), 6926-6935.

Nugroho, Priyo Puji. 2012. Pengembangan Model Single Sign-On untuk Layanan Internet dan Proxy IPB.

Nurul, S., Anggrainy, S., & Aprelyani, S., “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review SIM),” Jurnal Ekonomi Manajemen Sistem Informasi, 2022, 3(5), 564-573. https://doi.org/10.31933/jemsi.v3i5

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). Sistem keamanan informasi.

Prasetia, Y. A., & Manongga, D. (2024). Role-based access control (rbac) untuk sistem otorisasi terpusat berbasis flask studi kasus pt. xyz. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika), 9(4), 1768-1778.

Prasodi, B. A., Swastyastu, C. A., & Shanty, R. N. T. (2025). Implementasi Sistem Single Sign-On Berbasis Web Menggunakan Oauth2 Pada Sistem Informasi Di Universitas Dr. Soetomo. Journal of Informatics and Computer Science (JINACS), 6(03), 875-881. https://doi.org/10.26740/jinacs.v6n03.p875-881

Pratama, F., & Wicaksono, R. (2022). *Efisiensi Administrasi Hak Akses Berbasis Role-Based Access Control pada Lingkungan Organisasi*. Jurnal Sistem Informasi Universitas Muhammadiyah Jakarta, 5(1), 33–41..

Rasaputhra, S., Peiris, V., Magallagoda, R., Panditasekara, C., Wisenthige, K., & Jayasuriya, N. (2024). Do technological, environmental and entrepreneurial factors affect social commerce adoption? Journal of Small Business and Enterprise Development. https://doi.org/10.1108/JSBED-09-2023-0420

Ritonga, A., Togatorop, B. P. D., Ginting, H. B., Laoli, K. M., Sinaga, M. T. Y., & Amelia, R. I. (2025). Analisis Kombinatorik Dalam Menentukan Keamanan dan Kompleksitas Password dengan Penerapan Teori Kombinatorik. Katalis Pendidikan: Jurnal Ilmu Pendidikan dan Matematika, 2(2), 49-64.

Ru, R., Selo, S., & Widyawan, W. (2017). IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA PEMANFAATAN DATA KEPENDUDUKAN DITINGKAT KABUPATEN. Prosiding Semnastek.

Rusdan, M., & Sabar, M. (2020). Analisis dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication. Journal of Information Technology, 2(1), 17-24. https://doi.org/10.47292/joint.v2i1.20

Saputra, I. P., Utami, E., & Muhammad, A. H. (2022, October). Comparison of anomaly based and signature based methods in detection of scanning vulnerability. In 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 221-225). IEEE. https://doi.org/doi:10.23919/EECSI56542.2022.9946485

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. Jurnal Pendidikan Siber Nusantara, 1(2), 58–66.

Saputri, M. A., Pitrasacha Adytia, S. T., MT, P. I., Kom, B. S., & Kom, M. (2023). IMPLEMENTASI SINGLE SIGN ON (SSO) MENGGUNAKAN KEYCLOAK PADA SISTEM INFORMASI STMIK WIDYA CIPTA DHARMA. STMIK Widya Cipta Dharma.

Sari, A. P. Penerapan Autentikasi Dua Faktor (2FA) untuk Melindungi Data Pribadi pada Layanan Media Sosial. https://journal.uici.ac.id/index.php/stardia/article/view/15

Stallings, W. (2018). Kriptografi dan keamanan jaringan: Prinsip dan praktik (Edisi ke-7). Pearson.

Sahyudi, M., & Susanto, E. R. (2025). Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning. *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, 5(1), 105–116.

Sudiarto Raharjo, W., E.K. Ratri, I. D., & Susilo, H. (2017). Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login. Jurnal Teknik Informatika Dan Sistem Informasi, 3(1). https://doi.org/10.28932/jutisi.v3i1.579

Udayana, I. P. A. E. D., & Jasa, L. (2016). Implementasi Dan Analisis Single Sign On Pada Sistem Informasi Universitas Udayana. Semnasteknomedia Online, 4(1), 1-4. https://www.academia.edu/download/78561185/1105.pdf

Udayana, I. P. A. E. D., & Jasa, L. (2016). Implementasi Dan Analisis Single Sign On Pada Sistem Informasi Universitas Udayana. Semnasteknomedia Online, 4(1), 1-4. https://www.academia.edu/download/78561185/1105.pdf

Wahyudi, H., Zulianto, A., Maulana, A., Mardira Indonesia, S., & Langlangbuana, U. (2020). Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013 (Studi Kasus STMIK Mardira Indonesia) Heri. Jurnal Computech & Bisnis, Vol. 14 No(1), 40–46. https://doi.org/10.5281/zenodo.3929072

Wibowo, A. T., Slamet, S., Darwintha, H., & Pamuji, S. A. (2013). Implementasi Sistem Single Sign On (SSO) Terintegrasi Antara Captive Portal, STIKOM Apps dan Google Apps dalam Jaringan Wireless STIKOM Surabaya.

Wicaksono, H. R., Kabetta, H.,Hadiprakoso, R. B., & Qomariasih, N. (2025). Implementasi Single Sign-On (SSO) dengan Pendekatan Alaca's Framework untuk Peningkatan Keamanan Layanan Web Terintegrasi. JEPIN (Jurnal Edukasi dan Penelitian Informatika), 11(1), 18-26.

Yuricha, Y., & Phan, I. K. (2023). Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud: The Implementation of Role Based Access Control in a Cloud-Based Supply Chain Management System. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 3(2), 339–34