**Jurnal Manajemen Informatika Jayakarta**
Volume 4, Nomor 4, September 2024: halaman 396-403

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

# MANAJEMEN IDENTITAS DAN AKSES DALAM KEAMANAN SISTEM INFORMASI (PENDEKATAN LITERATURE REVIEW)

**[1]Cut Asiana Gemawaty*, [2] Yuce Yuliani**

[1,2] Program Studi Sistem Informasi, FILKOM, Universitas Gunadarma
Jl. Margonda Raya, Pondok Cina, Depok, Jawa Barat, Indonesia

*e-mail: cut_asiana@staff.gunadarma.ac.id

## Abstrak

Manajemen Identitas dan Akses (IAM) adalah elemen penting dalam memastikan keamanan sistem informasi dalam suatu organisasi. Penelitian ini bertujuan untuk mengeksplorasi konsep, teknik, dan implementasi IAM dalam konteks keamanan sistem informasi dengan menggunakan pendekatan literatur review. Dengan sistem federasi identitas dan Single Sign-On (SSO), organisasi dapat meningkatkan efisiensi dalam pengelolaan identitas pengguna dan akses ke berbagai aplikasi atau layanan tanpa memerlukan proses login berulang. Sistem federasi identitas memungkinkan pengguna untuk mengakses layanan dari berbagai organisasi dengan kredensial yang sama, mengurangi beban administrasi dan meningkatkan pengalaman pengguna. SSO, sebagai komponen utama IAM, memungkinkan pengguna mengakses beberapa aplikasi dengan satu kali login, yang mempermudah manajemen akses dan meningkatkan produktivitas. Namun, tantangan terkait keamanan tetap ada, terutama dalam hal risiko kebocoran data dan potensi serangan yang dapat mengeksploitasi kerentanannya. Penerapan teknologi keamanan seperti autentikasi multi-faktor dan pengelolaan akses berbasis peran dapat mengurangi potensi ancaman tersebut. Penelitian ini menyimpulkan bahwa IAM yang efektif sangat penting untuk keberlanjutan dan keamanan sistem informasi dalam organisasi modern.

**Kata kunci:** Manajemen Identitas, Manajemen Akses, Single Sign-On, Federasi Identitas, Keamanan Sistem Informasi

## *Abstract*

*Identity and Access Management (IAM) is a crucial element in ensuring the security of information systems within an organization. This study aims to explore the concepts, techniques, and implementations of IAM in the context of information system security through a literature review approach. With identity federation systems and Single Sign-On (SSO), organizations can improve efficiency in managing user identities and access to various applications or services without the need for repeated login processes. Identity federation allows users to access services from different organizations using the same credentials, reducing administrative burdens and enhancing user experience. SSO, as a core component of IAM, enables users to access multiple applications with a single login, simplifying access management and increasing productivity. However, security challenges remain, especially concerning data leakage risks and potential attacks exploiting its vulnerabilities. Implementing security technologies such as multi-factor authentication and role-based access management can mitigate such threats. This study concludes that effective IAM is essential for the continuity and security of information systems in modern organizations.*

**Jurnal Manajemen Informatika Jayakarta**
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

***Keywords:*** *Identity Management, Access Management, Single Sign-On, Identity Federation, Information System Security*

## Pendahuluan

Di era digital yang terus berkembang, sistem informasi menjadi tulang punggung berbagai aktivitas dalam bisnis, pemerintahan, pendidikan, hingga kehidupan sehari-hari. Keamanan sistem informasi memiliki peran penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data, sekaligus memastikan kelancaran operasional tanpa hambatan. Dengan meningkatnya ancaman keamanan, seperti akses tidak sah, peretasan, pencurian data, atau kerusakan sistem, perlindungan sistem informasi menjadi kebutuhan mendesak guna menjaga keberlanjutan organisasi dan melindungi keamanan nasional [1]. Keamanan sistem informasi didasarkan pada tiga pilar utama: Kerahasiaan *(Confidentiality*), Integritas *(Integrity*), dan Ketersediaan *(Availability)*. Untuk meningkatkan keamanan, berbagai strategi dapat diterapkan, seperti menggunakan enkripsi guna melindungi data sensitif, memasang firewall dan antivirus untuk mengelola lalu lintas jaringan serta mendeteksi malware, dan rutin memperbarui perangkat lunak untuk menutup potensi celah keamanan. Selain itu, membangun kesadaran akan pentingnya keamanan informasi di semua level, baik individu maupun organisasi, sangatlah krusial. Dengan demikian, setiap pihak dapat berkontribusi dalam membangun pertahanan yang kuat terhadap ancaman keamanan informasi [2].

Manajemen identitas dan akses (IAM) adalah elemen vital dalam keamanan sistem informasi, yang berfungsi melindungi data dan sumber daya organisasi dari akses tidak sah. Dengan semakin kompleksnya infrastruktur TI dan meningkatnya ancaman siber, organisasi perlu menerapkan strategi IAM yang efektif. Berdasarkan laporan *Cybersecurity & Infrastructure Security Agency* (CISA), lebih dari 90% pelanggaran data disebabkan oleh akses tidak sah, menegaskan pentingnya pengelolaan identitas yang lebih ketat [3].

Digital saat ini, di mana data menjadi aset yang sangat berharga, manajemen identitas dan akses (IAM) tidak hanya berfokus pada keamanan, tetapi juga memastikan kepatuhan terhadap regulasi yang berlaku. Sebagai contoh, *General Data Protection Regulation* (GDPR) di Eropa mengharuskan organisasi untuk menerapkan kontrol ketat atas akses ke data pribadi. Ketidakpatuhan terhadap regulasi ini dapat mengakibatkan sanksi berat, termasuk denda hingga 4% dari pendapatan tahunan global perusahaan [4]. Oleh karena itu, organisasi perlu memahami dan mengimplementasikan prinsip-prinsip IAM yang tidak hanya melindungi data, tetapi juga mendukung kepatuhan terhadap regulasi yang berlaku.

Manajemen Identitas dan Akses (IAM) memiliki peran vital dalam menjaga keamanan data dan sistem informasi di era digital. IAM dirancang untuk memastikan bahwa hanya individu yang terverifikasi dan memiliki izin yang sesuai yang dapat mengakses sumber daya, aplikasi, dan data sensitif. Dengan mengadopsi mekanisme otentikasi yang andal, seperti kata sandi kompleks dan autentikasi multi-faktor, organisasi dapat mengurangi risiko akses tidak sah. Selain itu, penerapan otorisasi yang sesuai memastikan pengguna hanya dapat mengakses informasi yang relevan dengan tugas atau tanggung jawab mereka, sehingga membantu mencegah potensi pelanggaran keamanan yang merugikan organisasi.

Implementasi manajemen identitas dan akses (IAM) juga berperan penting dalam mendukung kepatuhan terhadap regulasi privasi dan keamanan data, terutama di tengah meningkatnya ancaman siber. Dengan adanya sistem audit dan pemantauan yang terintegrasi, organisasi dapat memantau aktivitas pengguna serta mengidentifikasi upaya akses yang mencurigakan. Langkah ini tidak hanya memungkinkan deteksi pelanggaran keamanan secara cepat, tetapi juga menyediakan jejak audit yang berguna untuk analisis lanjutan. Secara keseluruhan, pengelolaan IAM yang efektif tidak hanya menjaga data sensitif tetap aman, tetapi juga meningkatkan efisiensi operasional dengan mempermudah proses manajemen pengguna dan pengaturan hak akses.

Implementasi manajemen identitas dan akses (IAM) dalam skala besar menghadirkan berbagai tantangan kompleks yang perlu dihadapi oleh organisasi. Salah satu kendala utama adalah pengelolaan izin dan akses yang semakin rumit seiring dengan berkembangnya jumlah pengguna,

**Jurnal Manajemen Informatika Jayakarta**
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

aplikasi, dan sumber daya yang harus diamankan. Dalam hal ini, organisasi harus menerapkan kebijakan akses yang konsisten dan efisien untuk memastikan bahwa setiap pengguna hanya mendapatkan akses sesuai dengan peran dan tanggung jawab mereka. Untuk itu, teknologi seperti kontrol akses berbasis atribut (ABAC) sering digunakan untuk menyederhanakan pengelolaan izin, memungkinkan penyesuaian akses secara dinamis berdasarkan atribut pengguna, tanpa perlu memperbarui izin secara manual setiap kali ada perubahan dalam struktur organisasi.

Selain itu, integrasi IAM dengan sistem dan aplikasi yang ada juga menjadi tantangan besar. Organisasi sering menggunakan berbagai platform dan layanan dengan mekanisme otentikasi dan otorisasi yang berbeda, yang dapat menyulitkan upaya untuk mempertahankan konsistensi dan keamanan di seluruh lingkungan. Untuk mengatasi hal ini, dibutuhkan pendekatan yang lebih terintegrasi dan otomatis dalam pengelolaan identitas serta akses, termasuk penerapan solusi berbasis cloud yang mampu mengelola skala besar secara efisien. Dengan demikian, meskipun tantangan implementasi IAM pada skala besar dapat menjadi hambatan, strategi yang tepat akan memungkinkan organisasi untuk meningkatkan keamanan data dan sistem mereka secara optimal [5].

Dalam konteks ini, artikel ini akan membahas berbagai aspek terkait manajemen identitas dan akses, termasuk tinjauan pustaka mengenai teori dan praktik terbaik, metode penelitian yang digunakan dalam kajian ini, hasil dan pembahasan yang diperoleh, serta kesimpulan yang dapat diambil dari analisis yang dilakukan. Diharapkan bahwa penelitian ini dapat memberikan wawasan yang lebih dalam mengenai pentingnya IAM dalam keamanan sistem informasi dan memberikan rekomendasi bagi praktik terbaik yang dapat diterapkan oleh organisasi.

## Tinjauan Literatur

Tinjauan pustaka ini akan mengulas berbagai literatur yang berkaitan dengan manajemen identitas dan akses, meliputi definisi, konsep dasar, serta perkembangan terkini dalam bidang ini. Manajemen identitas dan akses dapat dipahami sebagai suatu proses yang memastikan hanya individu yang berwenang yang memiliki akses ke sumber daya tertentu dalam sistem informasi [6]. Konsep ini mencakup serangkaian langkah penting seperti identifikasi, otentikasi, otorisasi, dan audit, yang semuanya berperan dalam melindungi data dan sistem.

Salah satu pendekatan yang sering dibahas dalam literatur adalah model kontrol akses berbasis peran *(Role-Based Access Control/RBAC).* Model ini memungkinkan organisasi memberikan hak akses berdasarkan peran pengguna dalam organisasi, sehingga dapat mengurangi kompleksitas dalam pengelolaan hak akses [6]. Penelitian oleh Hu et al. mengungkapkan bahwa penerapan RBAC dapat meningkatkan efisiensi dalam pengelolaan akses dan mengurangi potensi kesalahan manusia dalam penentuan hak akses [7]. Selain itu, perkembangan teknologi seperti penggunaan identitas digital dan sistem otentikasi multifaktor (MFA) juga merupakan topik yang sering dibahas dalam literatur. Menurut laporan dari Gartner, penggunaan MFA dapat mengurangi risiko pelanggaran akun hingga 99,9% [8]. Ini menunjukkan bahwa penerapan teknologi terbaru dalam IAM dapat memberikan perlindungan tambahan terhadap akses yang tidak sah.

Namun, meskipun banyak manfaat yang ditawarkan oleh sistem IAM, tantangan tetap ada. Salah satu tantangan utama adalah kebutuhan untuk menjaga keseimbangan antara keamanan dan kemudahan akses. Sebuah survei oleh Ponemon Institute menunjukkan bahwa 60% karyawan merasa bahwa langkah-langkah keamanan yang ketat mengganggu produktivitas mereka [9]. Oleh karena itu, penting bagi organisasi untuk merancang sistem IAM yang tidak hanya aman tetapi juga ramah pengguna.

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

## Metode Penelitian

Metode penelitian yang diterapkan dalam kajian ini adalah pendekatan tinjauan literatur, yang bertujuan untuk mengumpulkan, menganalisis, dan mensintesis informasi dari berbagai sumber yang relevan terkait manajemen identitas dan akses. Pendekatan ini dipilih karena memungkinkan peneliti memperoleh pemahaman yang lebih menyeluruh mengenai topik yang diteliti, serta mengidentifikasi tren dan pola yang mungkin tidak terlihat dalam studi yang lebih terfokus. Literatur yang digunakan dalam penelitian ini mencakup artikel jurnal, buku, laporan industri, serta dokumen kebijakan yang berhubungan dengan IAM.

Pendekatan ini bertujuan untuk menggali berbagai konsep dan praktik dalam manajemen identitas dan akses (Identity and Access Management/IAM) yang digunakan untuk meningkatkan keamanan sistem informasi. Fokus dari penelitian ini adalah untuk mengidentifikasi berbagai pendekatan, kebijakan, dan teknologi yang berhubungan dengan IAM, serta bagaimana hal ini mempengaruhi keamanan data dan perlindungan sistem informasi. Pendekatan kualitatif melalui literature review dalam manajemen identitas dan akses dalam keamanan sistem informasi memberikan gambaran komprehensif mengenai konsep-konsep utama, teknologi, dan tantangan yang ada. Dengan analisis tematik yang mendalam, pendekatan ini tidak hanya mengidentifikasi praktik terbaik, tetapi juga menyarankan arah untuk penelitian dan pengembangan lebih lanjut dalam bidang ini.

## Hasil

Manajemen Identitas dan Akses *(Identity and Access Management/IAM)* dalam konteks keamanan sistem informasi memainkan peran yang sangat penting dalam melindungi data dan sumber daya sistem dari akses yang tidak sah. Berdasarkan hasil telaah literatur yang ada, dapat diidentifikasi beberapa aspek penting dalam implementasi IAM yang efektif:

### Pentingnya Manajemen Identitas

Manajemen Identitas dan Akses (IAM) merupakan aspek krusial dalam keamanan informasi, terutama di era digital yang semakin terhubung. Berikut adalah beberapa poin penting mengenai peran dan manfaat IAM. IAM berfungsi untuk mencegah akses yang tidak sah ke sistem dan data sensitif. Dengan mengelola identitas dan akses pengguna secara tepat, organisasi dapat mengontrol siapa yang memiliki akses ke aplikasi, jaringan, dan sumber daya lainnya. Ini termasuk penerapan kebijakan keamanan seperti otentikasi multi-faktor dan enkripsi data, yang secara signifikan meningkatkan keamanan informasi. Dengan IAM, organisasi dapat membatasi akses hanya kepada pengguna yang sah dan memberikan hak akses sesuai kebutuhan. Ini membantu dalam mengidentifikasi dan mengurangi risiko serangan siber, pelanggaran data, serta pencurian informasi dengan memantau aktivitas pengguna secara terus-menerus [10]. Manajemen Identitas dan Akses (IAM) adalah landasan penting dalam strategi keamanan digital organisasi. Dengan mengelola identitas dan akses pengguna dengan baik, organisasi tidak hanya dapat meningkatkan keamanan tetapi juga memastikan kepatuhan terhadap regulasi serta meningkatkan efisiensi operasional. Oleh karena itu, investasi dalam solusi IAM yang efektif sangat diperlukan untuk melindungi aset digital di era modern ini.

### Pengelolaan Akses Berdasarkan Peran *(Role-Based Access Control - RBAC)*

Kontrol Akses Berbasis Peran (RBAC) adalah sistem manajemen akses yang mengatur hak akses pengguna berdasarkan peran mereka dalam suatu organisasi. Dalam pendekatan ini, administrator memberikan izin akses kepada pengguna berdasarkan tanggung jawab dan fungsi pekerjaan mereka, sehingga meminimalkan risiko akses tidak sah ke data sensitif dan sumber daya perusahaan. RBAC merupakan kombinasi dari dua model kontrol akses, yaitu Mandatory Access Control (MAC) dan Discretionary Access Control (DAC), yang memungkinkan pengelolaan hak akses secara lebih terstruktur dan efisien [11].

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

RBAC adalah metode yang efektif untuk mengelola kontrol akses dalam organisasi modern. Dengan menetapkan hak akses berdasarkan peran, bukan individu, RBAC membantu menjaga keamanan data dan mempermudah administrasi hak akses dalam lingkungan kerja yang dinamis. Implementasi RBAC juga mendukung kebijakan keamanan yang lebih luas dan memungkinkan adaptasi terhadap perubahan kebutuhan organisasi secara cepat dan efisien.

**Penerapan Kebijakan Akses dan Privasi**

Keamanan yang kuat memerlukan kebijakan yang jelas mengenai siapa yang boleh mengakses data dan sistem tertentu. Kebijakan ini termasuk pembatasan hak akses sesuai dengan prinsip kebutuhan untuk tahu (*need-to-know principle).* Implementasi kebijakan ini juga harus disertai dengan audit dan pelaporan akses secara berkala untuk memastikan bahwa kebijakan tersebut diterapkan dengan benar.

**Sistem Federasi Identitas dan Single Sign-On (SSO)**

Sistem Federasi Identitas merupakan pendekatan yang memungkinkan berbagai organisasi atau domain untuk berbagi dan mengelola informasi identitas pengguna tanpa perlu melakukan replikasi data. Dengan federasi identitas, sebuah organisasi dapat memberikan akses kepada pengguna dari organisasi lain untuk mengakses sumber daya tanpa harus membuat akun terpisah untuk setiap layanan atau aplikasi. Proses ini didukung oleh penggunaan protokol federasi standar seperti SAML *(Security Assertion Markup Language),* OAuth, atau OpenID Connect, yang memfasilitasi komunikasi dan pertukaran informasi identitas secara aman antar sistem yang berbeda.

Single Sign-On (SSO) adalah sistem yang memungkinkan pengguna untuk mengakses berbagai aplikasi atau layanan dengan hanya satu kali proses login. Setelah otentikasi pada aplikasi pertama (biasanya melalui Identity Provider), pengguna dapat langsung mengakses aplikasi atau layanan lainnya tanpa perlu login lagi. SSO mengurangi kebutuhan untuk mengingat banyak kata sandi, meningkatkan kenyamanan pengguna, serta mengurangi risiko yang terkait dengan penggunaan kata sandi yang lemah atau pengelolaan kredensial yang tidak aman.

**Keamanan Berbasis Cloud**

Cloud Security adalah pendekatan yang dirancang untuk melindungi infrastruktur, aplikasi, dan data yang disimpan dalam lingkungan cloud. Ini melibatkan berbagai langkah keamanan, seperti autentikasi pengguna, kontrol akses data, dan perlindungan privasi data. Dengan memanfaatkan teknologi seperti enkripsi dan firewall virtual, Cloud Security berperan dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Selain itu, model tanggung jawab bersama (shared responsibility model) menjadi kunci dalam hal ini, di mana penyedia layanan cloud bertanggung jawab atas keamanan infrastruktur, sementara pengguna bertanggung jawab atas data dan aplikasi yang mereka Kelola [12]. Namun, meskipun Cloud Security menawarkan banyak keuntungan seperti pengurangan biaya operasional dan peningkatan keandalan, tantangan tetap ada. Risiko keamanan seperti akses tidak sah dan pelanggaran data harus dikelola dengan baik. Oleh karena itu, perusahaan perlu menerapkan pilar-pilar keamanan yang kuat, termasuk manajemen identitas dan akses serta enkripsi data. Pemantauan berkelanjutan dan penilaian kerentanan juga penting untuk memastikan bahwa sistem tetap aman dari ancaman yang terus berkembang.

**Peran Teknologi Terbaru dalam IAM (Identity and Access Management)**

Teknologi terbaru, terutama dalam konteks Kecerdasan Buatan (AI) dan Internet of Things (IoT), memainkan peran penting dalam pengembangan dan implementasi sistem Identity and Access Management (IAM). IAM adalah kerangka kerja yang mengelola identitas digital pengguna dan akses ke sumber daya informasi dalam organisasi. Kecerdasan Buatan telah menjadi alat yang sangat berguna dalam memperkuat keamanan sistem IAM. Dengan kemampuannya untuk menganalisis pola perilaku pengguna, AI dapat mendeteksi aktivitas mencurigakan secara langsung. Sebagai contoh, jika seorang pengguna melakukan login dari lokasi yang tidak biasa atau mencoba mengakses data sensitif tanpa izin, sistem dapat segera mengeluarkan peringatan atau mengunci akun tersebut [13].

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

Teknologi otomatisasi memungkinkan organisasi untuk mengelola identitas pengguna dengan lebih efisien. Proses seperti provisioning dan deprovisioning akun pengguna dapat dilakukan secara otomatis, mengurangi risiko kesalahan manusia dan mempercepat waktu respons terhadap perubahan kebutuhan akses1. Ini sangat penting dalam lingkungan bisnis yang dinamis di mana karyawan sering berganti peran atau meninggalkan perusahaan. Dengan semakin banyaknya perangkat IoT yang terhubung, tantangan baru muncul dalam manajemen identitas dan akses. Teknologi terbaru memungkinkan integrasi perangkat IoT ke dalam sistem IAM, sehingga setiap perangkat dapat diidentifikasi dan dikelola dengan cara yang sama seperti pengguna manusia. Ini membantu memastikan bahwa hanya perangkat yang terautentikasi yang dapat mengakses jaringan dan data sensitive [14].

Teknologi biometrik, seperti pengenalan wajah dan sidik jari, semakin umum digunakan dalam sistem IAM. Metode ini menawarkan tingkat keamanan yang lebih tinggi dibandingkan dengan kata sandi tradisional, karena biometrik sulit untuk dipalsukan. Implementasi biometrik juga dapat meningkatkan pengalaman pengguna dengan mempercepat proses. Dengan adopsi layanan cloud, banyak organisasi kini menggunakan solusi IAM berbasis cloud yang menawarkan fleksibilitas dan skalabilitas lebih besar. Solusi ini memungkinkan pengelolaan identitas secara terpusat dan memberikan akses mudah bagi pengguna dari berbagai lokasi tanpa mengorbankan keamanan.

Seiring dengan kemajuan teknologi, penting untuk mempertimbangkan aspek etika dan kepatuhan dalam penerapan IAM. Organisasi harus memastikan bahwa penggunaan teknologi tidak melanggar privasi individu atau hukum yang berlaku. Pengembangan standar etis terkait penggunaan AI dan data identitas menjadi sangat penting untuk membangun kepercayaan antara pengguna dan penyedia layanan

## Pembahasan

### Tantangan dalam Implementasi IAM

Implementasi Identity and Access Management (IAM) menghadapi berbagai tantangan yang signifikan. Salah satu tantangan utama adalah kompleksitas pengelolaan akses di lingkungan yang terus berkembang, terutama dengan meningkatnya jumlah pengguna dan perangkat yang memerlukan akses ke sistem. Dengan banyaknya layanan cloud dan aplikasi yang digunakan, organisasi sering kali kesulitan untuk mengelola hak akses secara efektif, yang dapat mengakibatkan masalah seperti akses yang tidak sah atau penyalahgunaan hak akses. Selain itu, sistem IAM yang buruk dapat menyebabkan pelanggaran kebijakan keamanan dan ketidakpatuhan terhadap regulasi, berpotensi menimbulkan denda atau sanksi hukum bagi perusahaan.

Tantangan lain dalam penerapan IAM adalah mencapai keseimbangan antara keamanan dan produktivitas. Meskipun penting untuk menerapkan protokol keamanan yang ketat, terlalu banyak langkah autentikasi dapat mengganggu pengalaman pengguna dan menurunkan efisiensi. Sebagai contoh, penggunaan banyak kredensial atau kata sandi yang kompleks dapat menimbulkan frustrasi bagi karyawan. Oleh karena itu, organisasi perlu merancang dan merencanakan sistem IAM dengan hati-hati, memastikan bahwa proses autentikasi tetap aman namun tidak menghalangi kelancaran pekerjaan pengguna.

### Ancaman Terhadap Sistem IAM

Sistem Manajemen Identitas dan Akses (IAM) menghadapi berbagai ancaman yang dapat mengancam keamanan data dan integritas organisasi. Salah satu ancaman utama adalah pencurian identitas, di mana data pribadi atau keuangan milik karyawan atau pelanggan dicuri dan disalahgunakan untuk tujuan penipuan. Selain itu, serangan malware seperti virus dan ransomware dapat menginfeksi sistem IAM, merusak data, dan mencuri informasi sensitif. Ancaman lainnya termasuk serangan peretasan yang bertujuan untuk mengakses data secara ilegal, serta kesalahan manusia yang dapat menyebabkan pengaturan izin yang keliru atau kebocoran informasi [15]. Selain ancaman eksternal, terdapat juga risiko dari dalam organisasi, seperti kelalaian pengguna dan kolusi antara karyawan dengan pihak luar untuk melakukan pencurian data. Karyawan yang tidak sengaja mengungkapkan informasi sensitif atau menggunakan kata sandi yang lemah juga dapat membuka

Jurnal Manajemen Informatika Jayakarta
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

celah keamanan. Mengingat kompleksitas ancaman ini, penting bagi organisasi untuk menerapkan langkah-langkah keamanan yang ketat, termasuk autentikasi berlapis dan pemantauan aktivitas pengguna untuk melindungi sistem IAM dari berbagai risiko tersebut.

**Keterlibatan Pengguna dalam Keamanan IAM**

Keterlibatan pengguna dalam keamanan Identity and Access Management (IAM) sangat penting untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses sumber daya sistem, aplikasi, dan data sensitif. IAM mencakup beberapa komponen utama seperti otentikasi, yang memverifikasi identitas pengguna melalui berbagai metode seperti kata sandi atau sidik jari, dan otorisasi, yang menentukan hak akses berdasarkan peran dan tanggung jawab pengguna. Dengan manajemen identitas yang efektif, organisasi dapat mencegah akses tidak sah dan meminimalkan risiko pelanggaran keamanan. Selain itu, audit dan pengawasan aktivitas pengguna menjadi bagian integral dari IAM, membantu mendeteksi upaya akses yang mencurigakan dan memastikan kepatuhan terhadap kebijakan keamanan.

Pengguna juga berperan aktif dalam proses ini melalui praktik terbaik dalam penggunaan sistem IAM. Misalnya, mereka harus memahami pentingnya menjaga kerahasiaan kredensial mereka dan mengikuti prosedur onboarding serta offboarding yang tepat untuk memastikan bahwa hak akses diberikan dan dicabut sesuai kebutuhan. Implementasi kontrol akses berbasis peran (RBAC) memungkinkan organisasi untuk memberikan izin yang lebih terperinci kepada pengguna berdasarkan fungsi pekerjaan mereka, sehingga mengurangi risiko pemberian hak istimewa yang tidak perlu23. Dengan demikian, keterlibatan aktif pengguna dalam memahami dan mematuhi kebijakan IAM sangat penting untuk menciptakan lingkungan keamanan yang lebih kuat.

## Kesimpulan

Manajemen Identitas dan Akses (IAM) memiliki peran yang sangat penting dalam menjaga keamanan sistem informasi di dalam organisasi. Dengan menggunakan sistem federasi identitas dan Single Sign-On (SSO), organisasi dapat mempermudah pengelolaan akses dan identitas pengguna, serta meningkatkan pengalaman pengguna. Federasi identitas memungkinkan pengguna untuk mengakses layanan di berbagai organisasi dengan satu identitas yang terverifikasi, sementara SSO mempermudah pengguna dengan satu kali login untuk mengakses berbagai aplikasi. Meskipun demikian, tantangan dalam pengelolaan IAM tetap ada, terutama terkait dengan risiko kebocoran data dan ancaman dari serangan siber. Oleh karena itu, penerapan teknologi keamanan yang lebih kuat seperti autentikasi multi-faktor dan pengelolaan akses berbasis peran sangat penting untuk meningkatkan tingkat keamanan. Secara keseluruhan, implementasi IAM yang efektif dapat meningkatkan efisiensi, keamanan, dan produktivitas dalam organisasi, yang menjadikannya komponen vital dalam sistem informasi modern.

## Referensi

[1] PJJ Sistem informasi Universitas Siber Asia, “Mengamankan Sistem Informasi dalam Era Digital: Tantangan dan Strategi,” https://unsia.ac.id/author/sistem_informasi_admin/.
[2] A. Ramadhani, “Keamanan Informasi,” *Nusantara Journal of Information and Library Studies (N-JILS)*, vol. 1, no. 1, pp. 39–51, 2018.
[3] CISA., “‘Cybersecurity and Infrastructure Security Agency Annual Report.’”
[4] G. GDPR, “General data protection regulation,” *Regulation (EU)*, vol. 679, 2016.
[5] Z. Niqotaini, *Strategi Sistem Informasi*. 2024.
[6] R. S. Sandhu and P. Samarati, “Access control: principle and practice,” *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.
[7] V. C. Hu, D. F. Ferraiolo, R. Chandramouli, and D. R. Kuhn, *Attribute-Based Access Control*. Artech House, 2017.

**Jurnal Manajemen Informatika Jayakarta**
Volume 4, Nomor 4, September 2024: halaman 396-403
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v4i4.1527

[8] Gartner., *"Market Guide for Identity and Access Management."* 2023.
[9] Ponemon Institute., *"2023 Cost of a Data Breach Report."* 2023.
[10] Kania Sustisnawinata, "Identity and Access Management: Manfaat dan Pilar Utamanya," https://www.asdf.id/apa-itu-identity-and-access-management-iam/.
[11] Y. Prasetia, "ROLE-BASED ACCESS CONTROL (RBAC) UNTUK SISTEM OTORISASI TERPUSAT BERBASIS FLASK STUDI KASUS PT. XYZ," 2024.
[12] Ade Gusti, "Apa Itu Cloud Security dan Mengapa Penting di Era Digital Sekarang?," https://idwebhost.com/blog/tips-memilih-cloud-security/.
[13] M. R. R. Budianto, S. F. Kurnia, and T. R. S. W. Galih, "Perspektif Islam Terhadap Ilmu Pengetahuan dan Teknologi," *Islamika: Jurnal Ilmu-Ilmu Keislaman*, vol. 21, no. 01, pp. 55–61, 2021.
[14] A. Rukmana, "PERAN TEKNOLOGI DI DUNIA ISLAM," *Mumtaz: Jurnal Studi Al-Qur'an dan Keislaman*, vol. 2, pp. 111–120, Oct. 2019, doi: 10.36671/mumtaz.v2i1.21.
[15] L. A. Saputra, F. M. Akbar, F. Cahyaningtias, M. P. Ningrum, and A. Fauzi, "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," *Jurnal Pendidikan Siber Nusantara*, vol. 1, no. 2, pp. 58–66, 2023.