JUTIS (Jurnal Teknik Informatika Unis)
Vol. 13 No. 2 Bulan November 2025 **p-ISSN: 2252-5351**
Program Studi Teknik Informatika – Fakultas Teknik **e-ISSN: 2656-0860**
Universitas Islam Syekh-Yusuf Tangerang

Manajemen Identitas Dan Akses : Sebuah Analisis Mendalam Tentang Autentikasi, Otorisasi, Dan Manajemen Hidup Identitas

Muhammad Zaidan Rafat[1,*], Mursalin[2], Muhammad Rifki Maulana[3], Aan Anshori[4]
[1,2,3,4]Informatika, Fakultas Sains, UIN Sultan Maulana Hasanudin Banten, Sukajaya, 42171
*muhammadzaidanrafat@gmail.com [1], mursaalin90@gmail.com [2] , maulanarifqi741@gmail.com [3], aan.ansori@uinbanten.ac.id[4]

Abstrak
Manajemen identitas dan akses merupakan aspek krusial dalam keamanan informasi yang melibatkan proses autentikasi, otorisasi, dan pengelolaan identitas pengguna. Jurnal ini menganalisis berbagai metode 118ensiti akses, termasuk 118ensiti akses berbasis peran (RBAC) dan 118ensiti akses berbasis atribut (PBAC), yang digunakan untuk menentukan hak akses pengguna dalam sistem. Proses autentikasi, termasuk penerapan autentikasi dua 118ensit (2FA), diuraikan sebagai 118ensiti penting untuk memastikan keaslian identitas pengguna sebelum akses diberikan. Selain itu, jurnal ini menekankan pentingnya pemantauan dan audit berkala terhadap aktivitas pengguna untuk mendeteksi potensi penyalahgunaan. Dengan pendekatan yang sistematis terhadap manajemen identitas dan akses, organisasi dapat meningkatkan keamanan data dan melindungi informasi 118ensitive dari ancaman yang mungkin terjadi. Penelitian ini memberikan wawasan mendalam tentang praktik terbaik dalam manajemen identitas dan akses, serta tantangan yang dihadapi dalam implementasinya.

Kata kunci: *Manajemen Identitas, Kontrol Akses, Otentikasi, Otorisasi, Keamanan Informasi*

A. Pendahuluan

Manajemen Identitas dan Akses (IAM) telah menjadi komponen kunci dalam lanskap keamanan siber saat ini. Definisi yang jelas tentang IAM adalah sistem yang mengelola identitas digital dan penggunaan akses ke sumber daya organisasi secara efektif dan efisien. IAM mencakup dua komponen utama: manajemen identitas yang mengelola informasi identitas individu, dan manajemen akses yang mengatur siapa saja yang dapat mengakses sumber daya.

IAM sangat penting karena memungkinkan organisasi untuk mengontrol siapa saja yang memiliki akses ke sumber daya apa dan di bawah kondisi apa. Hal ini kritis dalam menjaga kerahasiaan data sensitif dan memastikan bahwa hanya pengguna yang sah saja yang dapat mengakses informasi konfidensial. Selain itu, IAM membantu organisasi mematuhi peraturan perlindungan data seperti GDPR dan PCI-DSS (Premsai, 2024).

Namun, implementasi IAM juga menghadapi tantangan utama. Dua tantangan utama adalah meningkatnya kompleksitas sistem IAM dengan pertumbuhan teknologi organisasi yang semakin beragam, serta biaya tinggi dalam mengembangkan dan

menjaga kinerja sistem IAM. Selain itu, risiko serangan siber terus meningkat, dengan biaya global dari insiden data breach mencapai $2.1 triliun pada tahun 2019 (Glöckler et al., 2023).

Penelitian ini bertujuan untuk menyelidiki lebih lanjut terkait autentikasi, otorisasi, dan manajemen hidup identitas dalam konteks IAM. Kepenulisan ini akan mengupas lebih dalam mengenai teknologi dalam IAM, seperti single sign on (SSO), Multi-Factor Authentication (MFA), Privileged access management (PAM). Diharapkan kepenulisan ini dapat memberikan wawasan terkini terkait Manajemen Identitas dan Akses, beserta teknologinya.

B. Metode

Metode Penelitian ini menggunakan metode berupa studi literature, Metode ini melibatkan proses sistematis dalam mengidentifikasi, mengevaluasi, dan menginterpretasikan semua penelitian yang relevan dengan topik atau pertanyaan penelitian tertentu.

Gambar 1. Alur Metode Penelitian

C. Hasil dan Pembahasan

Manajemen Identitas dan Akses atau *Identity Access Management* (IAM) adalah praktik yang memastikan bahwa hanya orang dan entitas dengan identitas digital yang memiliki level peran dan izin akses yang sesuai agar dapat mengakses sumber daya perusahaan seperti jaringan dan basis data. Izin akses dan peran pengguna ditetapkan dan dikelola melalui sistem IAM. Banyak organisasi menggunakan IAM sebagai kunci untuk mengatasi masalah keamanan siber (Mohammed, 2015).

IAM digunakan untuk melawan akses data yang tidak sah dan ancaman yang mungkin terjadi saat aktivitas jarak jauh. Fokus IAM adalah pada keamanan data, autentikasi, otorisasi, sinkronisasi data, manajemen kontak pelanggan, dan privasi. Komponen dasar IAM termasuk manajemen identitas, otentikasi melalui password, token, atau biometrik, otorisasi berdasarkan peran, serta audit untuk mendeteksi akses yang tidak sah..

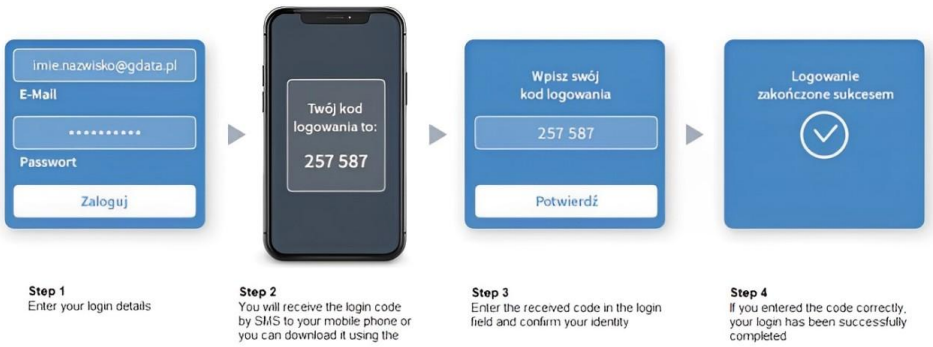
Manajemen Identitas dan Akses (IAM) telah mengalami evolusi signifikan sejak awal kemunculannya hingga perkembangan terkini. Awalnya, IAM hanya berfokus pada mekanisme autentikasi dasar seperti username dan password untuk mengontrol akses ke sistem. Namun seiring berkembangnya teknologi dan meningkatnya ketergantungan bisnis pada sistem digital, kebutuhan akan IAM mulai berkembang menjadi sistem yang lebih lengkap dan canggih. Dengan semakin banyaknya data yang disimpan secara digital dan akses yang diperlukan dari berbagai lokasi, organisasi

p-ISSN: 2252-5351
e-ISSN: 2656-0860

mulai menerapkan solusi IAM yang lebih canggih. Fitur seperti *Single Sign-On* (SSO), autentikasi multi-faktor, dan kontrol akses adaptif diperkenalkan untuk meningkatkan keamanan dan efisiensi dalam pengelolaan identitas.

Authentication atau otentikasi adalah proses pemeriksaan suatu identitas guna melakukan validasi ke aslian identitas tersebut guna masuk ke dalam sistem (Saputra et al., 2021). Autentikasi dua faktor (2FA) telah menjadi standar keamanan dasar bagi banyak organisasi dalam beberapa tahun terakhir. Meskipun menawarkan peningkatan keamanan yang signifikan dibandingkan otentikasi satu faktor, 2FA juga memiliki dampak pada pengalaman pengguna yang perlu dipertimbangkan. Autentikasi Dua Faktor (2FA) adalah metode keamanan yang memerlukan pengguna untuk menyediakan dua bentuk identitas verifikasi sebelum diberi akses ke suatu sistem atau layanan (Suleski et al., 2023). 2FA dirancang untuk meningkatkan keamanan dibandingkan dengan autentikasi satu faktor tradisional yang hanya menggunakan kata sandi saja.

Namun penting untuk diperhatikan bahwa Autentikasi Dua Faktor (2FA) tidak diaktifkan secara default dan harus diaktifkan oleh pengguna. Selain itu, banyak aplikasi yang tidak mendukung login dengan autentikasi dua faktor untuk layanan online. Ilustrasi cara kerja 2FA menggunakan kode SMS diberikan pada gambar 1.



Gambar 2. Ilustrasi cara kerja 2FA

Proses ini biasanya membutuhkan nama pengguna dan kata sandi, sama seperti platform lainnya. Namun, setelah memasukkan kredensial ini, pengguna juga harus memiliki *smartphone*, untuk menyelesaikan bagian kedua dari verifikasi, yang dikenal sebagai Autentikasi Dua Faktor (2FA) (Florczak et al., 2023). Ada dua metode utama untuk menggunakan ponsel selama proses login. Langkah pertama adalah mendaftarkan nomor telepon ke Google. Ketika pengguna mencoba masuk dengan nama pengguna dan kata sandi mereka, Google mengirimkan kode unik melalui SMS yang harus dimasukkan ke ponsel. Metode kedua melibatkan pemasangan aplikasi otentikasi Google pada ponsel pengguna, yang menghasilkan kode unik. Metode ini memiliki keuntungan karena tidak memerlukan koneksi jaringan, karena kode dibuat langsung pada perangkat.

Selain daripada mekanisme autentikasi 2FA, Autentikasi Biometrik telah berkembang menjadi metode autentikasi yang kuat dan unik dalam beberapa dekade terakhir. Autentikasi Biometrik sendiri dapat berupa fisiologis seperti sidik jari, wajah,

iris, suara, retina, ciri perilaku, atau tanda tangan (Warda Hassan & Nosheen Sabahat, 2024).

Data biometrik digunakan untuk mengidentifikasi dan mengautentikasi orang dengan menggunakan karakteristik unik mereka. Hal ini dilakukan dengan mengambil karakteristik pengguna sebagai masukan dan mencocokkannya dengan data yang tersimpan dalam data biometrik pengguna untuk mendeteksi kemiripan (Liskin et al., 2020). Jika ditemukan kesamaan, maka orang tersebut teridentifikasi, jika tidak, maka tidak. Data biometrik tidak selalu seragam karena orang berubah, misalnya pada wajah, rambut wajah bisa tumbuh, untuk mata, kacamata atau lensa bisa dipakai, dll. Adapun pengaplikasian serta permasalahan autentikasi biometrik yang disajikan dalam tabel berikut ;

Tabel 1. Pengaplikasian Biometrik

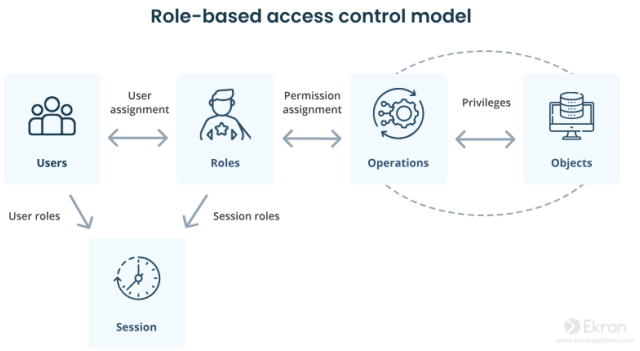
No	Teknik	Pengaplikasian	Masalah	Dasar Pemikiran
1.	Sidik Jari	Smartphone, deteksi kejahatan, Sistem Kehadiran, Industri Keamanan	Elastisitas Kulit Pengolahan Kelembaban Kerutan	Deformasi, Verifikasi yang cepat
2.	Pemindaian Wajah	Smartphone, keamanan perangkat, cctv, & forensik	Gerakan, Pencahayaan, Penyamaran	Variasi, penerangan, Perubahan Ketidakkonsistenan
3.	Iris Mata	Manajemen identitas, border control	Kacamata, silau	Obstruksi, refleksi
4.	Retina	Instalasi Militer, Fasilitas Nuklir	Patologi, fobia	DegradasiLaser
5.	Suara	Smartphone, Customer Service, IOT	Noise, Dialect	Hambatan, akurasi

Dalam mekanisme Otorisasi IAM, terdapat sebuah terdapat sebuah model yang bernama *Role-Based Access Control* (RBAC). Model ini bertidak sebagai model kontrol akses yang menggunakan peran atau role sebagai dasar untuk mengatur hak akses pengguna dalam sistem informasi. Dalam RBAC, aktivitas sistem dan izin akses sumber daya dikaitkan dengan peran tertentu, bukan langsung diberikan kepada pengguna individu. Komponen inti RBAC meliputi pengguna (*users*), objek (*objects*), peran (*roles*), izin (*permissions*), dan sesi (*sessions*) (Mohamed et al., 2022). Peran bertindak sebagai lapisan intermediate antara subjek dan hak akses. Penugasan pengguna ke peran dapat berubah seiring waktu, sedangkan penugasan peran ke izin relatif lebih stabil.

Adapun alur kerja dari mekanisme *Role-Based Access Control* (RBAC) secara umum yang dimulai dari : a) Pendefinisian peran: Administrator sistem mendefinisikan peran-peran yang ada dalam organisasi, seperti manajer, karyawan, atau auditor ; b) Penugasan pengguna ke peran: Pengguna diassign ke peran tertentu berdasarkan fungsi atau posisi mereka dalam organisasi; c) Pemberian izin akses: Izin akses diberikan kepada peran, bukan langsung kepada pengguna; d)Pembuatan sesi: Ketika pengguna login, sistem menciptakan sesi aktif yang merepresentasikan peran yang dimiliki pengguna tersebut; e) Pengambilan keputusan akses: Sistem memutuskan apakah pengguna dapat melakukan tindakan tertentu berdasarkan peran yang dimilikinya. Ilustrasi dapat dilihat

p-ISSN: 2252-5351
e-ISSN: 2656-0860

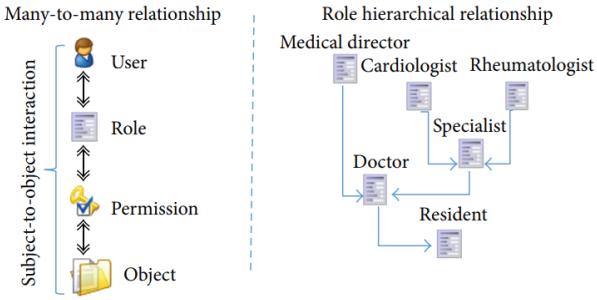
pada gambar 2.



Gambar 3. Alur kerja RBAC
Sumber : https://www.syteca.com/en/blog/rbac-vs-abac

Model *Role-Based Access Control* (RBAC) terdiri dari inti, hirarkis, pemisahan statis, dan pemisahan dinamis dalam hubungan tugas. Model ini mengelola kebijakan keamanan organisasi dengan efektif. Izin peran dalam RBAC terkait dengan sesi pengguna, dengan keputusan otorisasi berdasarkan pemetaan objek. Model ini mencegah duplikasi izin antar grup berkat sifat hirarkisnya. Satu peran dapat terhubung dengan peran lain, memungkinkan fleksibilitas akses yang lebih luas. Sebuah pengguna dapat memiliki beberapa peran, menyediakan kontrol akses yang efisien. Hubungan antara pengguna, peran, dan izin menjadi lebih terstruktur dan efisien dalam RBAC.

Dalam ilustrasi (Gambar 3), direktur medis, ahli jantung, dan ahli reumatologi berbagi set izin dokter dan residen. Ahli jantung dan ahli reumatologi berbagi izin spesialis. Ketiganya memiliki set izin mereka sendiri. Pemisahan komponen tugas secara statis dan dinamis dapat digunakan untuk mengelompokkan otoritas di antara pengguna yang berbeda untuk lebih memperketat otorisasi untuk menolak dengan cara tertentu sehingga tindakan yang dibatasi tidak dapat dilakukan sendiri oleh satu pengguna sistem.



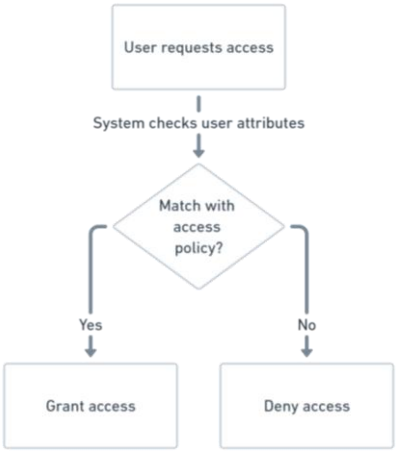
Gambar 4. RBAC Hierarki
Sumber : (De Carvalho Junior & Bandiera-Paiva, 2018)

Selain *Role-Based Access Control* RBAC, terdapat satu mekanisme otorisasi yaitu Model akses berbasis kebijakan (*Policy-Based Access Control*, PBAC), yang mana model ini merupakan pendekatan yang semakin penting dalam pengelolaan akses ke sumber daya dalam sistem informasi. PBAC memungkinkan pengaturan hak akses yang lebih fleksibel dan dinamis dibandingkan dengan model tradisional seperti *Discretionary Access Control*

(DAC), *Mandatory Access Control* (MAC), dan *Role-Based Access Control* (RBAC) (Pan et al., 2021). Secara umum PBAC, mendefinisikan kebijakan akses berdasarkan kebutuhan organisasi dan konteks operasional. Kebijakan ini dapat mencakup berbagai faktor seperti identitas pengguna, atribut lingkungan, dan jenis data yang diakses. Kebijakan ini sering kali ditulis dalam format yang dapat dipahami oleh sistem, seperti XML atau JSON, dan dapat mencakup aturan yang kompleks yang menggabungkan berbagai kondisi (Bhatt et al., 2021).

Ketika permintaan akses diajukan, sistem PBAC akan mengevaluasi kebijakan yang relevan untuk menentukan apakah permintaan tersebut memenuhi syarat untuk akses. Proses ini melibatkan pemeriksaan atribut pengguna dan kondisi yang ditetapkan dalam kebijakan. Jika semua syarat terpenuhi, akses dapat diberikan; jika tidak, akses akan ditolak (Lacroix & Boucelma, 2013). Setelah evaluasi, jika permintaan akses disetujui, sistem akan memberikan izin akses kepada pengguna. Proses ini dapat melibatkan pengeluaran token akses atau pembaruan status dalam sistem untuk mencerminkan izin yang baru diberikan (Sarath Tomy, 2016).

Dalam ilustrasi pada (Gambar 4), seorang pengguna meminta akses ke suatu sumber daya. Kemudian sistem akan memeriksa atribut pengguna dan mencocokkannya dengan kebijakan akses yang telah ditetapkan. Jika sesuai, pengguna akan diizinkan mengakses sumber daya tersebut. Ini menunjukkan pentingnya aturan akses dalam menentukan siapa yang boleh mengakses suatu sumber daya dan dalam kondisi apa.



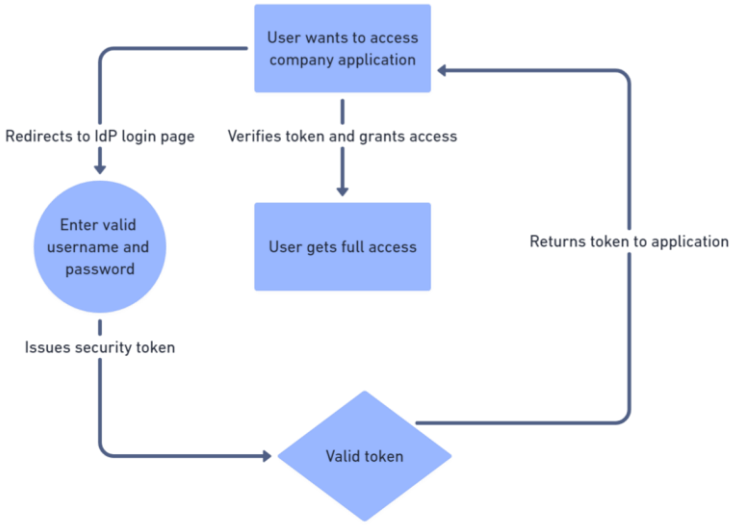
Gambar 5. Alur kerja PBAC sederhana

Dalam hal Manajemen Identitas dan Akses, *Single-Sign On* (SSO) berfungsi untuk menyederhanakan proses autentikasi dan meningkatkan pengalaman pengguna dengan mengurangi jumlah kata sandi yang perlu diingat dan dikelola (Milenković et al., 2013; Waluyo & Sutarman, 2022). SSO sendiri merupakan mekanisme autentikasi yang memungkinkan pengguna untuk mengakses berbagai aplikasi dan layanan dengan hanya satu set kredensial, SSO bekerja dengan cara mengautentikasi pengguna sekali melalui penyedia identitas (*Identity Provider*, IdP) dan kemudian memberikan akses ke berbagai aplikasi atau layanan tanpa perlu autentikasi ulang (Aldaoud et al., 2024; Pavani, 2018).

Dalam ilustrasi pada (Gambar 5), dijelaskan bahwa Diagram alur kerja SSO

p-ISSN: 2252-5351
e-ISSN: 2656-0860

menggambarkan proses autentikasi tunggal yang memungkinkan pengguna mengakses berbagai aplikasi perusahaan dengan hanya satu kali login. Ketika pengguna mencoba masuk ke sebuah aplikasi, mereka akan diarahkan ke halaman login Identity Provider (IdP). Setelah memasukkan kredensial yang valid, IdP akan mengeluarkan token keamanan. Token ini kemudian dikirim ke aplikasi yang diminta dan diverifikasi. Jika token valid, pengguna akan diberikan akses penuh ke aplikasi tersebut.



Gambar 6. Alur kerja SSO

Dalam Manajemen identitas dan Akses, Proses *provisioning* pengguna baru dalam sebuah organisasi merupakan serangkaian langkah untuk menyediakan akses dan hak akses bagi pengguna baru agar dapat menggunakan sistem dan layanan yang disediakan oleh organisasi. Peran *Identity Provider* (IdP) dan *Service Provider* (SP) dalam proses ini sangat penting untuk memastikan provisioning berjalan dengan aman dan efisien.

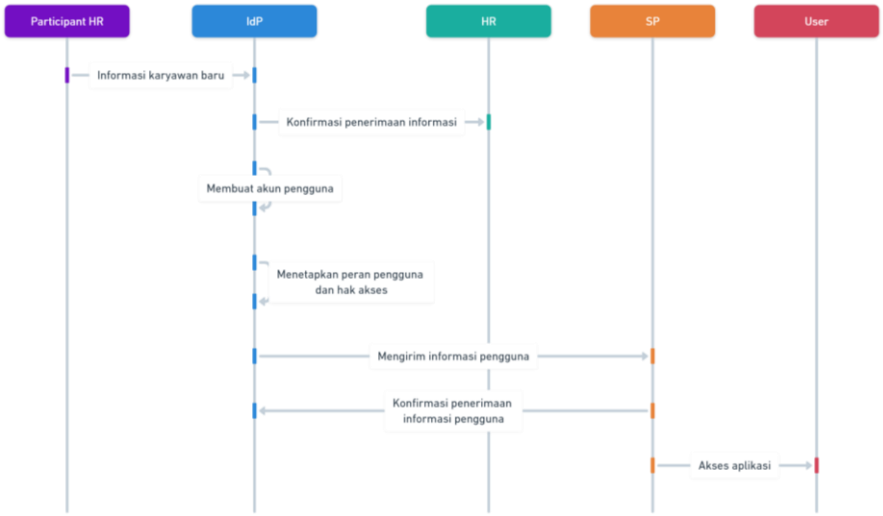
Pertama, peran IdP adalah untuk mengelola identitas pengguna dan memberikan otentikasi yang aman. IdP bertanggung jawab untuk memverifikasi identitas pengguna dan memberikan token akses yang dapat digunakan oleh SP untuk memberikan akses ke layanan (Demchenko & De Laat, 2011). Sementara itu, SP bertanggung jawab untuk menyediakan layanan yang dibutuhkan oleh pengguna dan memastikan akses yang diberikan sesuai dengan otorisasi yang dimiliki.

Praktik terbaik untuk memastikan provisioning yang aman dan efisien meliputi penerapan proses onboarding standar yang terdokumentasi, integrasi IdP dan SP menggunakan protokol standar, kontrol akses berbasis peran, pemantauan aktivitas pengguna secara berkala, mekanisme self-service, dan proses deprovisioning efektif saat pengguna keluar dari organisasi. Ini penting untuk mencegah potensi penyalahgunaan akses dan memastikan keamanan informasi yang sensitif.

Alur diagram pada (Gambar 6) menjelaskan proses pemberian akses akun pengguna baru di sistem, dimulai dari informasi karyawan baru yang diterima oleh HR dan diverifikasi oleh *Identity Provider* (IdP). IdP akan membuat akun pengguna sesuai dengan data karyawan baru dan menetapkan peran serta hak akses yang sesuai. Setelah

p-ISSN: 2252-5351
e-ISSN: 2656-0860

itu, IdP akan mengirimkan informasi pengguna lengkap kepada Service Provider (SP) untuk dikonfirmasi. Setelah konfirmasi, pengguna baru dapat mengakses aplikasi atau sistem yang telah dialokasikan kepadanya dengan menggunakan kredensial login yang telah diberikan. Mereka dapat mulai menjalankan tugas sesuai dengan peran dan hak akses yang telah ditetapkan.



Gambar 7. Diagram Alur Provisioning

Selain Provisioning, dalam Manajemen Identitas dan Akses terdapat Deprovisioning. Yang mana Deprovisioning sendiri merupakan proses penghapusan atau penonaktifan akses pengguna terhadap sistem informasi dan sumber daya organisasi. Proses ini sangat krusial dalam menjaga keamanan sistem informasi karena dapat mencegah penyalahgunaan akses oleh pengguna yang tidak lagi membutuhkannya. Deprovisioning berbeda dengan provisioning, yang merupakan proses pemberian akses baru kepada pengguna, dan disabling akun, yang hanya menonaktifkan akun tanpa menghapus akses.

Dalam proses deprovisioning pengguna, organisasi sering menghadapi beberapa tantangan, seperti data remanence dan risiko akses tidak sah. Data remanence mengacu pada keberadaan data yang masih tersisa setelah penghapusan atau deprovisioning pengguna, yang dapat menyebabkan kebocoran informasi sensitif (Mollakuqe & Dimitrova, 2024). Selain itu, risiko akses tidak sah juga menjadi perhatian utama, di mana mantan pengguna dapat tetap memiliki akses ke sumber daya organisasi bahkan setelah deprovisioning (Jalili et al., 2019).

Gambar 7 menunjukkan diagram alur proses deprovisioning untuk pengguna Active Directory, yang mencakup: a). Tahap Persiapan: Transfer aset digital (seperti dokumen, proyek, dll.) ke pengguna lain atau arsip; b. Tahap Deactivasi: Menonaktifkan akun pengguna Active Directory, termasuk reset password dan cookie; c). Tahap Manajemen Grup: Menghapus pengguna dari semua grup distribusi dan menambahkannya ke grup keamanan untuk pengguna yang dinonaktifkan; d). Menghaspus akun; e). Tahap Manajemen Email: Mengelola akun email pengguna,

p-ISSN: 2252-5351
e-ISSN: 2656-0860

termasuk mengarsipkan kotak masuk dan mengatur balasan otomatis; f). Tahap Finalisasi: Memverifikasi bahwa semua akses pengguna telah dihapus dan akun telah benar-benar dinonaktifkan..

Gambar 8. Diagram alur proses deprovisioning

D. Kesimpulan

Penelitian ini berhasil menunjukkan bahwa manajemen identitas dan akses (IAM) memainkan peran yang sangat penting dalam meningkatkan keamanan siber organisasi. Temuan menunjukkan bahwa penerapan sistem IAM yang efektif, termasuk penggunaan kontrol akses berbasis peran (RBAC) dan kontrol akses berbasis atribut (PBAC), dapat secara signifikan mengurangi risiko pelanggaran data dan penyalahgunaan akses. Selain itu, penerapan metode autentikasi yang lebih canggih, seperti autentikasi multi-faktor, terbukti meningkatkan keandalan proses verifikasi identitas pengguna. Dengan demikian, tujuan penelitian untuk mengeksplorasi praktik terbaik dalam IAM dan tantangan yang dihadapi dalam implementasinya telah tercapai. Penelitian ini juga menegaskan bahwa pemantauan dan audit yang berkelanjutan terhadap aktivitas pengguna adalah kunci untuk mendeteksi dan mencegah potensi ancaman. Secara keseluruhan, hasil penelitian ini mendukung hipotesis bahwa sistem IAM yang terintegrasi dan canggih dapat memberikan perlindungan yang lebih baik terhadap data sensitif dan memastikan kepatuhan terhadap regulasi perlindungan data.

Daftar Pustaka

Aldaoud, M., Al-abri, D., Kausar, F., & Awadalla, M. (2024). NDNOTA : NDN One-Time Authentication. *Information*, *15*, 1–18. https://doi.org/https://doi.org/10.3390/info15050289

Bhatt, S., Pham, T. K., Gupta, M., Benson, J., Park, J., & Sandhu, R. (2021). Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future. *IEEE Access*, *9*, 107200–107223. https://doi.org/10.1109/ACCESS.2021.3101218

De Carvalho Junior, M. A., & Bandiera-Paiva, P. (2018). Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of Healthcare Engineering*, *2018*. https://doi.org/10.1155/2018/6510249

Demchenko, Y., & De Laat, C. (2011). Defining generic architecture for cloud infrastructure as a service model. *Proceedings of Science*, 1–10.

Florczak, S., Jasiak, A., & Szczygieł, I. (2023). Two-Factor Authentication (2Fa) Comparison of Methods and Applications. *Advances in Web Development Journal*, *1*(3), 26–45.

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business and Information Systems Engineering*, *66*(4), 421–440. https://doi.org/10.1007/s12599-023-00830-x

Jalili, V., Afgan, E., Taylor, J., Goecks, J., & Health, O. (2019). *Cloud Bursting Galaxy : Federated Identity and Access Management*. 1–10. https://doi.org/10.1101/506238

Lacroix, J., & Boucelma, O. (2013). Provenance-based access control in the cloud. *Proceedings - IEEE 10th International Conference on Services Computing, SCC 2013*, 755–756. https://doi.org/10.1109/SCC.2013.51

Liskin, V., Serdobolskiy, E., Sopilko, I., & Okhrimenko, T. (2020). Two-factor user authentication using biometrics. *CEUR Workshop Proceedings*, *2654*, 526–535. CEUR-WS.org/Vol-2654/paper41.pdf

Milenković, I., Latinović, O., & Simić, D. (2013). Using Kerberos protocol for Single Sign-On in Identity Management Systems. *JITA - Journal of Information Technology and Applications (Banja Luka) - APEIRON*, *5*(1), 27–33. https://doi.org/10.7251/jit1301027m

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*, *18*(2–3), 156–180. https://doi.org/10.1108/IJWIS-04-2022-0077

Mohammed, I. A. (2015). The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study. *International Journal of Creative Research Thoughts - IJCRT*, *3*(1), 2320–2882. www.ijcrt.org

Mollakuqe, E., & Dimitrova, V. (2024). Comparative analysis of identity management , access control , and authorization practices in public and private. *Open Research Europe*. https://doi.org/10.12688/openreseurope.16634.2

Pan, R., Wang, G., & Wu, M. (2021). An Attribute-Based Access Control Policy Retrieval Method Based on Binary Sequence. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/5582921

Pavani, V. L. (2018). A novel authentication mechanism to prevent unauthorized service access for mobile device in distributed network. *International Journal of Interactive Mobile Technologies*, *12*(8), 4–19. https://doi.org/10.3991/ijim.v12i8.8194

Premsai, R. (2024). A Comprehensive Framework for Cybersecurity in Identity and Access Management Systems. *Journal of Mathematical & Computer Application*, *3*(2), 1–6. https://doi.org/doi.org/10.47363/JMCA/2024(3)E140

Saputra, I. P., Yusuf, R., & Saprudin, U. (2021). Implementasi Cloud Computing Sebagai Radius Server Pada Jaringan Internet Router Mikrotik. *Journal Computer Science and Informatic Systems : J-Cosys*, *1*(2), 94–100. https://doi.org/10.53514/jc.v1i2.67

Sarath Tomy, E. P. (2016). Controlling Privacy Disclosure of Third Party Applications in Online Social Networks Article information : To cite this document : About Emerald www.emeraldinsight.com Emerald is a global publisher linking research and practice to the benefit of society . *International Journal of Web Information Systems*, *12*. https://doi.org/https://doi.org/10.1108/IJWIS-12-2015-0045

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*. https://doi.org/10.1177/20552076231177144

Waluyo, T., & Sutarman. (2022). Comparative Analysis of the Performance of Single Sign-On Authentication Systems with OpenID and OAuth Protocols. *International Journal of Computer and Information Technology(2279-0764)*, *11*(3), 100–107. https://doi.org/10.24203/ijcit.v11i3.277

Warda Hassan, & Nosheen Sabahat. (2024). Towards Secure Identification: A Comparative Analysis of Biometric Authentication Techniques. *VFAST Transactions on Software Engineering*, *12*(1), 105–120. https://doi.org/10.21015/vtse.v12i1.1745