JURNAL TAMPIASIH
INSTITUT TEKNOLOGI DAN KESEHATAN ASPIRASI
E-ISSN : 2986 - 8742

Implementasi Access Control pada Sistem Informasi Akuntansi untuk Meningkatkan Keamanan Data Keuangan

Muhammad Innuddin[1], Muliani[2],
[1]Akuntansi, Universitas Bumigora Mataram, Indonesia
[2]Teknologi Informasi, Institut Teknologi dan Kesehatan Aspirasi, Indonesia

Email : muhammadinnuddin@universitasbumigora.ac.id[1] , muliani@universitasbumigora.ac.id[2]

ABSTRAK

Keamanan data keuangan merupakan salah satu aspek penting dalam pengembangan Sistem Informasi Akuntansi karena data tersebut bersifat sensitif dan berhubungan langsung dengan aktivitas operasional organisasi. Penelitian ini bertujuan mengimplementasikan Access Control berbasis Role-Based Access Control (RBAC) untuk membatasi akses pengguna sesuai dengan tugas dan kewenangannya. Metode penelitian menggunakan pendekatan System Development Life Cycle (SDLC) yang meliputi analisis kebutuhan, perancangan, implementasi, pengujian, dan evaluasi. Sistem dirancang dengan beberapa peran pengguna, yaitu administrator, bendahara, kasir, pimpinan, dan auditor, dengan hak akses yang berbeda terhadap transaksi dan laporan keuangan. Pengujian dilakukan menggunakan *black-box testing* dan skenario pengujian otorisasi untuk memastikan pengguna hanya dapat mengakses fungsi dan data yang telah diberikan. Hasil penelitian menunjukkan bahwa penerapan access control dapat memperkuat pembatasan akses terhadap data keuangan, mengurangi peluang perubahan data oleh pengguna yang tidak memiliki kewenangan, serta menyediakan jejak aktivitas melalui *audit log*. Implementasi tersebut mendukung prinsip kerahasiaan, integritas, dan ketersediaan data sehingga keamanan Sistem Informasi Akuntansi dapat ditingkatkan.

Kata Kunci: Access Control, RBAC, Sistem Informasi Akuntansi, Keamanan Data, Audit Log.

ABSTRACT

Financial data security is a critical aspect of developing an Accounting Information System, given the sensitive nature of the data and its direct link to an organization's operational activities. This study aims to implement Role-Based Access Control (RBAC) to restrict user access based on specific duties and authority levels. The research employs the System Development Life Cycle (SDLC) methodology, encompassing requirements analysis, design, implementation, testing, and evaluation. The system is designed with distinct user roles—administrator, treasurer, cashier, management, and auditor—each with specific access rights regarding financial transactions and reports. Testing was conducted using black-box testing and authorization scenarios to ensure users could access only those functions and data for which they were authorized. The results demonstrate that implementing access control strengthens restrictions on financial data, minimizes the risk of unauthorized data modification, and provides an activity trail via audit logs. This implementation supports the principles of data confidentiality, integrity, and availability, thereby enhancing the security of the Accounting Information System.

Keywords: *Access Control, RBAC, Accounting Information System, Data Security, Audit Log.*

***Corresponding author:** muhammadinnuddin@universitasbumigora.ac.id

PENDAHULUAN

Sistem Informasi Akuntansi (SIA) merupakan bagian penting dalam pengelolaan informasi organisasi karena digunakan untuk mengelola berbagai aktivitas keuangan, mulai dari pencatatan transaksi, penerimaan dan pengeluaran kas, pengelolaan piutang dan utang, sampai penyusunan laporan keuangan. Perkembangan teknologi informasi menyebabkan proses akuntansi semakin banyak dilakukan menggunakan aplikasi berbasis komputer maupun web. Kondisi tersebut memberikan manfaat berupa peningkatan kecepatan pemrosesan, kemudahan pencarian data, pengurangan pekerjaan manual, serta tersedianya informasi keuangan secara lebih cepat untuk mendukung pengambilan keputusan. Namun, digitalisasi juga menyebabkan data keuangan menjadi bagian dari aset informasi yang harus mendapatkan perlindungan memadai. Data keuangan dapat mengandung informasi transaksi, nilai pembayaran, identitas pihak yang melakukan transaksi, informasi rekening, dan informasi internal organisasi sehingga akses terhadap data tersebut tidak seharusnya diberikan kepada seluruh pengguna secara bebas. Apabila mekanisme keamanan tidak dirancang dengan baik, pengguna yang telah berhasil melakukan login dapat memperoleh akses terhadap fungsi atau data yang sebenarnya berada di luar kewenangannya. Oleh karena itu, autentikasi saja tidak cukup untuk menjamin keamanan aplikasi karena autentikasi hanya membuktikan identitas pengguna, sedangkan otorisasi menentukan apakah pengguna tersebut diperbolehkan melakukan tindakan tertentu. OWASP menjelaskan bahwa pengguna yang berhasil diautentikasi belum tentu memiliki hak untuk mengakses seluruh sumber daya aplikasi. (Mercado et al., n.d.) Dalam konteks Sistem Informasi Akuntansi, pemisahan antara autentikasi dan otorisasi menjadi sangat penting karena pengguna dengan peran berbeda memiliki tanggung jawab yang berbeda pula. Administrator membutuhkan hak pengelolaan pengguna dan konfigurasi sistem, bendahara membutuhkan akses terhadap aktivitas keuangan tertentu, kasir membutuhkan akses terhadap transaksi operasional, pimpinan membutuhkan akses terhadap laporan, sedangkan auditor membutuhkan akses untuk pemeriksaan tanpa harus memiliki kewenangan mengubah transaksi. Apabila seluruh pengguna diberikan hak akses yang sama, risiko penyalahgunaan maupun kesalahan operasional dapat meningkat. Dengan demikian, sistem informasi akuntansi membutuhkan mekanisme pengendalian akses yang mampu menerjemahkan struktur organisasi dan pembagian tugas ke dalam aturan teknis pada aplikasi.

Salah satu model pengendalian akses yang sesuai untuk kebutuhan tersebut adalah Role-Based Access Control (RBAC). Pada RBAC, hak akses dikaitkan dengan peran tertentu dan pengguna memperoleh hak tersebut berdasarkan peran yang diberikan kepadanya. Konsep ini memungkinkan organisasi mengelola hak akses secara lebih terstruktur dibandingkan pemberian hak satu per satu kepada setiap pengguna. NIST menjelaskan bahwa pada model RBAC, peran membawa sekumpulan hak akses tertentu dan pengguna diberikan peran tersebut sehingga keputusan akses dapat ditentukan berdasarkan peran yang dimiliki. (Force, 2020) Dalam implementasi pada Sistem Informasi Akuntansi, RBAC dapat digunakan untuk membentuk hubungan antara pengguna, peran, menu, fungsi, dan data. Misalnya, administrator dapat mengelola pengguna, bendahara dapat memasukkan dan memverifikasi transaksi tertentu, kasir dapat melakukan pencatatan transaksi operasional, pimpinan dapat melihat laporan, dan auditor dapat membaca data serta aktivitas sistem. Pengaturan tersebut dapat diperluas menjadi pengendalian pada tingkat fungsi maupun objek data sehingga tidak hanya menu yang dibatasi, tetapi juga operasi *create*, *read*, *update*, dan *delete* (CRUD). Prinsip *least privilege* menjadi bagian penting dalam desain tersebut, yaitu setiap pengguna hanya diberikan hak minimum yang diperlukan untuk menjalankan tugasnya. OWASP juga merekomendasikan penerapan *least privilege*, *deny by default*, pemeriksaan otorisasi pada

setiap permintaan, serta pencatatan aktivitas otorisasi. (Rakshit, 2022) Dengan pendekatan tersebut, keamanan tidak hanya bergantung pada tampilan antarmuka. Sistem harus melakukan validasi otorisasi pada sisi server agar pengguna tidak dapat memperoleh hak akses tambahan hanya dengan memanipulasi URL, parameter, atau permintaan aplikasi. Pemeriksaan pada sisi server sangat penting karena pemeriksaan yang hanya dilakukan pada sisi klien dapat dilewati dan tidak boleh menjadi dasar utama pemberian hak akses.

Permasalahan lain yang perlu diperhatikan adalah kemampuan sistem dalam mencatat aktivitas pengguna. Pembatasan akses akan lebih efektif apabila setiap aktivitas penting dapat ditelusuri melalui audit log. Audit log dapat mencatat identitas pengguna, waktu aktivitas, jenis aktivitas, objek yang diakses, dan hasil aktivitas. Dalam Sistem Informasi Akuntansi, mekanisme tersebut dapat digunakan untuk membantu mengetahui siapa yang memasukkan transaksi, siapa yang melakukan perubahan, siapa yang menghapus data, serta kapan aktivitas tersebut dilakukan. Pencatatan tersebut juga mendukung proses pemeriksaan apabila terjadi ketidaksesuaian antara transaksi dengan kondisi sebenarnya. OWASP merekomendasikan agar kejadian otorisasi dicatat dan pengujian terhadap aturan otorisasi dilakukan melalui *unit test* maupun *integration test*. (Rojabi, 2025) Selain itu, keamanan data tidak dapat dipandang hanya dari aspek kerahasiaan. Sistem juga harus mempertahankan integritas agar data tidak diubah oleh pihak yang tidak memiliki kewenangan serta ketersediaan agar informasi dapat digunakan oleh pengguna yang sah ketika diperlukan. NIST Cybersecurity Framework 2.0 memberikan kerangka pengelolaan risiko keamanan siber yang dapat digunakan organisasi untuk memahami, menilai, memprioritaskan, dan mengomunikasikan risiko keamanan. (Pascoe et al., 2024) Oleh karena itu, implementasi access control pada sistem informasi akuntansi perlu dirancang sebagai bagian dari mekanisme keamanan secara menyeluruh, bukan sekadar fitur login. Pengendalian harus mencakup identifikasi pengguna, pembentukan peran, pemberian permission, validasi otorisasi, pembatasan akses terhadap data, pencatatan aktivitas, serta pengujian terhadap kemungkinan pelanggaran hak akses. Pendekatan tersebut dapat memberikan lapisan perlindungan yang lebih baik terhadap aset informasi keuangan.

Berdasarkan permasalahan tersebut, penelitian ini berfokus pada implementasi Access Control pada Sistem Informasi Akuntansi untuk meningkatkan keamanan data keuangan. Penelitian diarahkan untuk merancang mekanisme RBAC yang dapat menghubungkan pengguna dengan peran dan hak akses tertentu, kemudian menerapkannya pada fungsi utama sistem informasi akuntansi. Penelitian juga memasukkan audit log sebagai mekanisme pendukung untuk merekam aktivitas penting pengguna. Tujuan penelitian adalah menghasilkan mekanisme pengendalian akses yang dapat memastikan bahwa pengguna hanya dapat menjalankan aktivitas sesuai dengan kewenangannya, mencegah akses terhadap fungsi yang tidak diizinkan, serta meningkatkan kemampuan sistem dalam melakukan penelusuran aktivitas pengguna. Penelitian ini juga melakukan pengujian terhadap beberapa skenario akses, seperti akses yang diizinkan, akses yang ditolak, percobaan membuka halaman tertentu secara langsung, perubahan data oleh pengguna yang tidak memiliki hak, dan aktivitas setelah pengguna keluar dari sistem. Pendekatan tersebut diharapkan dapat menunjukkan bahwa penerapan access control dapat menjadi salah satu mekanisme penting untuk meningkatkan keamanan Sistem Informasi Akuntansi. Penelitian ini memiliki kontribusi pada aspek teknis karena menghasilkan rancangan hubungan antara role dan permission, serta kontribusi praktis karena memberikan model pengendalian akses yang dapat diterapkan pada aplikasi akuntansi berbasis web. Dengan demikian, penelitian tidak hanya menghasilkan sistem yang dapat digunakan untuk mengolah transaksi keuangan, tetapi juga sistem yang memperhatikan prinsip keamanan informasi melalui pembatasan hak akses, pemisahan kewenangan, dan pencatatan aktivitas pengguna.

METODE PENELITIAN

Penelitian ini menggunakan metode System Development Life Cycle (SDLC) sebagai pendekatan pengembangan sistem. SDLC digunakan karena penelitian tidak hanya menganalisis konsep keamanan, tetapi juga merancang, mengimplementasikan, dan menguji mekanisme access control pada Sistem Informasi Akuntansi. Tahapan penelitian terdiri atas analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi. Pada tahap analisis kebutuhan dilakukan identifikasi terhadap proses bisnis akuntansi, jenis pengguna, fungsi sistem, jenis data yang dikelola, serta risiko keamanan yang mungkin terjadi. Data kebutuhan dapat diperoleh melalui observasi terhadap proses pengelolaan keuangan, wawancara dengan pengguna sistem, dokumentasi proses bisnis, dan studi literatur. Fokus analisis diarahkan pada aktivitas yang memiliki hubungan dengan data keuangan, seperti pengelolaan akun pengguna, pencatatan transaksi, pengelolaan data pelanggan atau pemasok, pengelolaan penerimaan dan pengeluaran, serta penyusunan laporan. Selanjutnya dilakukan identifikasi terhadap kebutuhan keamanan berdasarkan prinsip kerahasiaan, integritas, dan ketersediaan. Prinsip *least privilege* digunakan sebagai dasar dalam menentukan hak akses sehingga pengguna tidak diberikan hak yang tidak dibutuhkan. OWASP merekomendasikan bahwa akses sebaiknya ditolak secara default apabila tidak ada aturan yang secara eksplisit mengizinkannya.(Mercado et al., n.d.) Analisis juga mencakup identifikasi terhadap kemungkinan *privilege escalation*, akses langsung terhadap URL, manipulasi parameter, dan penggunaan akun yang tidak lagi memiliki kewenangan. Hasil analisis kemudian digunakan sebagai dasar penyusunan kebutuhan fungsional dan kebutuhan keamanan sistem.

Tahap kedua adalah perancangan access control. Model yang digunakan adalah Role-Based Access Control (RBAC) dengan struktur utama berupa *user*, *role*, *permission*, dan *resource*. Setiap pengguna memiliki satu atau lebih peran sesuai kebutuhan organisasi, sedangkan setiap peran memiliki kumpulan permission yang menentukan tindakan yang dapat dilakukan. Permission dapat didefinisikan dalam bentuk operasi *create*, *read*, *update*, dan *delete* terhadap objek tertentu. Sebagai contoh, role administrator dapat memiliki permission mengelola pengguna dan konfigurasi sistem, role bendahara dapat memiliki permission terhadap transaksi keuangan, role kasir memiliki permission terhadap transaksi operasional, role pimpinan memiliki permission membaca laporan, dan role auditor memiliki permission membaca data dan audit log. Struktur tersebut dapat direpresentasikan dalam basis data melalui tabel *users*, *roles*, *permissions*, *user_roles*, dan *role_permissions*. Selain pembatasan berdasarkan fungsi, desain juga dapat diterapkan pada tingkat objek sehingga pengguna hanya dapat melihat atau mengubah data yang sesuai dengan kewenangannya. NIST menjelaskan bahwa RBAC menggunakan peran yang membawa sekumpulan hak tertentu dan mekanisme pengendalian mengevaluasi peran pengguna terhadap operasi yang diminta pada objek. (Grassi et al., 2020) Dalam perancangan ini, aturan *deny by default* diterapkan untuk memastikan bahwa permission yang belum diberikan tidak dapat digunakan. Mekanisme pemeriksaan otorisasi dirancang pada sisi server sehingga pembatasan tidak hanya bergantung pada tampilan menu. Setiap permintaan terhadap sumber daya dilanjutkan dengan proses pemeriksaan identitas dan permission sebelum sistem memberikan respons. Pendekatan tersebut sejalan dengan rekomendasi OWASP yang menekankan pemeriksaan otorisasi terhadap setiap permintaan dan penerapan *least privilege*.

Tahap ketiga adalah implementasi sistem. Implementasi dilakukan dengan membangun modul autentikasi, modul manajemen role, modul permission, modul transaksi, modul laporan, dan modul audit log. Pada modul autentikasi, sistem melakukan validasi identitas pengguna sebelum memberikan sesi akses. Setelah berhasil login, sistem membaca role pengguna dan permission

yang terkait. Ketika pengguna meminta suatu fungsi, sistem melakukan pemeriksaan apakah permission tersebut tersedia pada role pengguna. Jika permission tersedia, permintaan diproses; apabila tidak tersedia, sistem menolak permintaan dan mencatat kejadian tersebut. Implementasi harus memastikan bahwa validasi tidak hanya dilakukan pada antarmuka pengguna. Sebagai contoh, meskipun menu “Manajemen Pengguna” tidak ditampilkan kepada pengguna dengan role kasir, server tetap harus menolak permintaan apabila pengguna mencoba mengakses endpoint tersebut secara langsung. OWASP secara eksplisit menekankan bahwa pemeriksaan access control harus dilakukan pada sisi server, gateway, atau mekanisme serverless dan tidak boleh bergantung pada pemeriksaan sisi klien. Audit log kemudian digunakan untuk mencatat aktivitas keamanan penting, termasuk login, logout, kegagalan login, akses yang ditolak, pembuatan transaksi, perubahan transaksi, dan penghapusan data apabila fungsi tersebut memang diperbolehkan. Data audit log dapat meliputi *user ID*, role, waktu, alamat atau informasi sesi yang relevan, jenis aktivitas, objek data, dan status aktivitas. Pada tahap ini juga diterapkan mekanisme pengelolaan sesi, validasi input, perlindungan terhadap manipulasi parameter, serta pengelolaan akun yang sudah tidak aktif. Implementasi tersebut dimaksudkan untuk membangun pengendalian berlapis sehingga access control tidak menjadi satu-satunya mekanisme keamanan.

Tahap terakhir adalah pengujian dan evaluasi. Pengujian dilakukan menggunakan Black Box Testing dengan fokus pada fungsi autentikasi, otorisasi, pembatasan menu, pembatasan transaksi, dan audit log. Selain itu, dilakukan pengujian khusus access control untuk memastikan bahwa pengguna tidak dapat mengakses fungsi di luar role-nya. Skenario pengujian mencakup login menggunakan akun valid, login menggunakan kredensial tidak valid, akses terhadap menu sesuai role, akses terhadap menu yang tidak sesuai role, akses langsung melalui URL, manipulasi parameter identitas data, percobaan melakukan operasi CRUD tanpa permission, dan akses setelah sesi berakhir. Hasil setiap pengujian dikategorikan menjadi “diizinkan” atau “ditolak” sesuai dengan aturan permission yang telah dirancang. Pengujian juga dilakukan terhadap audit log untuk memastikan aktivitas penting tercatat secara konsisten. Evaluasi dilakukan dengan membandingkan kondisi sebelum dan sesudah penerapan access control berdasarkan indikator seperti jumlah fungsi yang dapat diakses pengguna, kemampuan sistem menolak akses tidak sah, kemampuan mencatat aktivitas, dan kesesuaian antara role dengan permission. Pengujian otorisasi penting karena kelemahan access control dapat memungkinkan pengguna yang telah terautentikasi melakukan aktivitas yang sebenarnya tidak diperbolehkan. OWASP menempatkan pengujian aturan otorisasi sebagai bagian penting dari pengembangan sistem yang aman. Selanjutnya, hasil pengujian dianalisis secara deskriptif untuk mengetahui efektivitas mekanisme access control dalam memenuhi kebutuhan keamanan sistem informasi akuntansi.

HASIL DAN PEMBAHASAN

Hasil implementasi menunjukkan bahwa mekanisme access control dapat digunakan untuk membentuk pembagian hak akses yang lebih terstruktur pada Sistem Informasi Akuntansi. Sistem dirancang dengan lima role utama, yaitu administrator, bendahara, kasir, pimpinan, dan auditor. Administrator memiliki kewenangan paling luas terhadap konfigurasi sistem dan pengelolaan akun, tetapi tetap perlu dibatasi berdasarkan kebutuhan operasional. Bendahara diberikan akses terhadap proses keuangan yang menjadi tanggung jawabnya, sedangkan kasir diberikan akses terhadap transaksi operasional yang berkaitan dengan aktivitas kas. Pimpinan diberikan akses membaca informasi dan laporan yang diperlukan untuk pengambilan keputusan tanpa diberikan hak untuk mengubah transaksi. Auditor diberikan akses untuk melakukan pemeriksaan terhadap data dan aktivitas sistem tanpa diberikan kewenangan untuk memodifikasi data transaksi. Pembagian tersebut menghasilkan matriks role dan permission yang dapat menjadi dasar pengendalian akses.

Konsep tersebut sesuai dengan RBAC, yaitu hak akses dikaitkan dengan role dan pengguna mendapatkan privilege melalui role yang dimilikinya. Implementasi ini juga menerapkan prinsip *least privilege*, sehingga pengguna hanya memperoleh hak yang dibutuhkan untuk menyelesaikan tugasnya. Dengan demikian, apabila terjadi kesalahan akun atau kredensial pengguna diketahui pihak lain, cakupan akses yang dapat digunakan tetap dibatasi oleh permission role tersebut. Pembatasan ini penting terutama pada sistem yang mengelola data keuangan karena pengguna yang bertugas mencatat transaksi tidak selalu membutuhkan hak untuk mengubah konfigurasi pengguna atau menghapus seluruh data. Sistem juga menerapkan *deny by default*, sehingga fungsi yang tidak memiliki permission tidak dapat digunakan. Pendekatan tersebut mengurangi ketergantungan terhadap asumsi bahwa semua pengguna merupakan pengguna terpercaya.

Hasil pengujian access control menunjukkan bahwa mekanisme otorisasi dapat memisahkan akses berdasarkan fungsi dan role. Pengujian dilakukan dengan memberikan beberapa akun simulasi kepada masing-masing role, kemudian menjalankan sejumlah skenario akses. Akun administrator dapat mengakses fungsi pengelolaan pengguna dan konfigurasi, sedangkan akun kasir tidak dapat mengakses fungsi tersebut. Akun pimpinan dapat membuka laporan keuangan tetapi tidak dapat melakukan perubahan terhadap transaksi. Akun auditor dapat membaca informasi yang diperlukan untuk pemeriksaan, sedangkan fungsi perubahan atau penghapusan transaksi ditolak. Pengujian juga mencakup akses langsung terhadap alamat halaman yang tidak tersedia pada menu pengguna. Dalam kondisi tersebut, sistem tidak hanya menyembunyikan menu, tetapi melakukan pemeriksaan permission di server dan mengembalikan respons penolakan ketika pengguna tidak memiliki hak. Mekanisme ini penting karena menyembunyikan menu saja bukan merupakan mekanisme keamanan yang memadai. OWASP menegaskan bahwa pemeriksaan access control harus dilakukan pada sisi server karena pemeriksaan sisi klien dapat dilewati. Pengujian terhadap akses data juga menunjukkan bahwa aturan permission perlu diterapkan pada tingkat objek, bukan hanya pada halaman. Misalnya, pengguna dapat memiliki akses ke halaman transaksi tetapi hanya boleh melihat atau mengubah transaksi tertentu sesuai kewenangannya. Pengujian semacam ini membantu mengurangi risiko *broken access control*, termasuk kondisi ketika pengguna yang telah login dapat mengakses objek milik pengguna lain hanya dengan mengubah identifier. Dengan menerapkan pemeriksaan permission pada setiap permintaan, sistem dapat memastikan bahwa keputusan akses tidak hanya berdasarkan status login, tetapi berdasarkan hubungan antara pengguna, role, permission, operasi, dan sumber daya yang diminta.

Implementasi audit log memberikan hasil tambahan berupa kemampuan penelusuran aktivitas pengguna. Sistem mencatat aktivitas seperti login berhasil, login gagal, logout, akses yang ditolak, penambahan transaksi, perubahan transaksi, dan aktivitas administrasi tertentu. Informasi tersebut memberikan jejak yang dapat digunakan untuk proses audit dan investigasi internal apabila terjadi ketidaksesuaian data. Sebagai contoh, apabila suatu transaksi berubah, administrator atau auditor dapat memeriksa identitas pengguna yang melakukan perubahan, waktu perubahan, dan jenis aktivitas yang dilakukan. Audit log juga dapat digunakan untuk mengidentifikasi pola aktivitas yang tidak biasa, seperti percobaan berulang mengakses fungsi yang tidak memiliki permission. OWASP merekomendasikan pencatatan kejadian otorisasi dan penggunaan pengujian untuk memverifikasi aturan akses aplikasi. Dalam konteks keamanan data keuangan, audit log memberikan lapisan *accountability* karena aktivitas dapat dikaitkan dengan akun tertentu. Namun, audit log harus dirancang agar tidak mudah dimanipulasi oleh pengguna biasa. Hak untuk melihat, mengubah, atau menghapus log perlu dibatasi secara ketat. Bahkan administrator sebaiknya tidak diberikan kemampuan menghapus catatan audit secara sembarangan tanpa prosedur yang jelas. Selain itu, data log perlu dikelola agar tidak menyimpan informasi sensitif secara berlebihan. Hasil tersebut menunjukkan bahwa access control dan audit log memiliki hubungan yang saling mendukung:

access control membatasi tindakan pengguna, sedangkan audit log menyediakan informasi mengenai aktivitas yang telah terjadi. Kombinasi keduanya memberikan pengendalian yang lebih kuat dibandingkan penggunaan autentikasi saja.

Dari sisi keamanan informasi, implementasi access control memberikan kontribusi terhadap tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan ditingkatkan melalui pembatasan pengguna terhadap data dan fungsi yang tidak menjadi kewenangannya. Integritas ditingkatkan dengan mencegah pengguna yang tidak memiliki permission melakukan perubahan atau penghapusan transaksi. Ketersediaan tetap dijaga dengan memastikan pengguna yang sah dapat mengakses fungsi sesuai kebutuhan operasional. Penerapan tersebut sejalan dengan pendekatan pengelolaan risiko keamanan siber yang menempatkan pengendalian identitas, akses, dan perlindungan aset informasi sebagai bagian dari pengelolaan keamanan secara keseluruhan. NIST CSF 2.0 memberikan kerangka untuk membantu organisasi memahami dan mengelola risiko keamanan siber, meskipun framework tersebut tidak menentukan satu metode implementasi teknis tertentu. Hasil penelitian juga menunjukkan bahwa RBAC merupakan pilihan yang efektif untuk organisasi yang struktur tugasnya relatif jelas karena administrator dapat mengelola permission berdasarkan role tanpa menetapkan hak akses secara individual untuk setiap pengguna. Namun, RBAC bukan berarti seluruh persoalan keamanan telah selesai. Organisasi tetap membutuhkan pengelolaan siklus hidup akun, peninjauan permission secara berkala, penghapusan atau penonaktifan akun yang tidak digunakan, pengamanan sesi, pengujian keamanan, dan pemantauan log. Untuk kebutuhan yang lebih kompleks, model berbasis atribut seperti Attribute-Based Access Control (ABAC) dapat dipertimbangkan karena keputusan akses dapat mempertimbangkan atribut pengguna, objek, operasi, dan kondisi lingkungan. NIST SP 800-162 menjelaskan bahwa ABAC menentukan otorisasi dengan mengevaluasi atribut subjek, objek, operasi yang diminta, dan dalam kondisi tertentu atribut lingkungan terhadap kebijakan atau aturan. (Hu et al., 2014) Dengan demikian, hasil penelitian menunjukkan bahwa implementasi RBAC dapat menjadi fondasi access control pada Sistem Informasi Akuntansi, sedangkan pengembangan berikutnya dapat mengombinasikannya dengan pendekatan berbasis atribut untuk kebutuhan organisasi yang lebih dinamis.

KESIMPULAN

Berdasarkan hasil perancangan dan implementasi, dapat disimpulkan bahwa Access Control merupakan komponen penting dalam meningkatkan keamanan Sistem Informasi Akuntansi. Sistem yang hanya menggunakan autentikasi belum cukup untuk memastikan bahwa pengguna hanya dapat melakukan aktivitas sesuai dengan kewenangannya. Penerapan Role-Based Access Control (RBAC) memungkinkan sistem menghubungkan pengguna dengan role tertentu dan memberikan permission berdasarkan tugas masing-masing. Pada penelitian ini, role administrator, bendahara, kasir, pimpinan, dan auditor memiliki hak akses yang berbeda terhadap menu, fungsi, dan data sistem. Pembagian tersebut membantu mengurangi pemberian hak akses secara berlebihan serta mendukung prinsip *least privilege*. Sistem juga menerapkan konsep *deny by default*, sehingga pengguna tidak memperoleh hak akses terhadap fungsi yang belum diberikan permission. Pendekatan tersebut sesuai dengan rekomendasi keamanan aplikasi yang menekankan pembatasan akses berdasarkan kebutuhan dan pemeriksaan otorisasi secara konsisten. Dengan demikian, implementasi access control tidak hanya menjadi fitur tambahan pada sistem, tetapi menjadi mekanisme yang menghubungkan struktur kewenangan organisasi dengan aturan keamanan aplikasi.

Hasil pengujian menunjukkan bahwa mekanisme access control mampu membedakan aktivitas yang diizinkan dan ditolak berdasarkan role pengguna. Pengguna dapat menjalankan fungsi sesuai dengan permission yang dimilikinya, sedangkan akses terhadap fungsi yang tidak sesuai dengan kewenangan ditolak oleh sistem. Pemeriksaan juga dapat diterapkan pada akses langsung terhadap halaman atau endpoint sehingga keamanan tidak hanya bergantung pada tampilan menu. Hal tersebut penting karena pengguna yang telah berhasil login belum tentu memiliki hak untuk menggunakan seluruh fungsi sistem. OWASP membedakan autentikasi dan otorisasi serta menekankan bahwa pemeriksaan authorization harus dilakukan pada sisi server. Dengan adanya mekanisme tersebut, risiko perubahan data keuangan oleh pengguna yang tidak berwenang dapat diminimalkan. Selain itu, penerapan pembatasan akses berdasarkan role dapat membantu organisasi menerapkan pemisahan tugas (*separation of duties*), misalnya membedakan pihak yang melakukan pencatatan transaksi, pihak yang melakukan pemeriksaan, dan pihak yang menggunakan laporan untuk pengambilan keputusan. Pemisahan tersebut dapat mengurangi risiko konflik kepentingan dan kesalahan operasional dalam pengelolaan data keuangan.

Penerapan audit log juga memberikan kontribusi terhadap keamanan karena aktivitas pengguna dapat ditelusuri. Sistem dapat mencatat aktivitas login, logout, akses yang ditolak, pembuatan transaksi, perubahan data, dan aktivitas administratif tertentu. Informasi tersebut dapat dimanfaatkan untuk audit internal, pemantauan keamanan, serta investigasi apabila terjadi ketidaksesuaian data. Dengan demikian, sistem tidak hanya melakukan pencegahan melalui access control, tetapi juga menyediakan mekanisme *accountability* melalui pencatatan aktivitas. Meskipun demikian, audit log harus dilindungi dari perubahan atau penghapusan yang tidak sah dan perlu dikelola sesuai dengan kebutuhan organisasi. Penelitian ini juga menunjukkan bahwa pengamanan sistem informasi akuntansi harus dilakukan secara berlapis. Access control perlu dikombinasikan dengan pengamanan autentikasi, pengelolaan sesi, validasi input, pengamanan basis data, pencadangan data, pemantauan log, dan pengujian keamanan secara berkala. Kerangka keamanan seperti NIST CSF 2.0 dapat digunakan sebagai referensi untuk mengelola risiko keamanan siber secara lebih menyeluruh.

Untuk pengembangan penelitian selanjutnya, mekanisme RBAC dapat dikembangkan menjadi pendekatan yang lebih dinamis dengan mengombinasikannya dengan Attribute-Based Access Control (ABAC). ABAC memungkinkan keputusan akses mempertimbangkan atribut pengguna, objek, operasi, dan kondisi lingkungan sehingga lebih sesuai untuk organisasi yang mempunyai aturan akses kompleks. (Hu et al., 2014) Penelitian berikutnya juga dapat menambahkan autentikasi multifaktor, enkripsi data sensitif, *security monitoring*, *penetration testing* yang terkontrol, serta analisis anomali terhadap audit log. Pengujian dapat diperluas menggunakan OWASP Web Security Testing Guide dan pengujian otomatis terhadap aturan authorization. Dengan pengembangan tersebut, Sistem Informasi Akuntansi tidak hanya memiliki mekanisme pembatasan akses berdasarkan role, tetapi juga mempunyai kemampuan mendeteksi, mencatat, dan merespons aktivitas keamanan secara lebih komprehensif. Secara keseluruhan, penelitian ini menunjukkan bahwa implementasi access control berbasis RBAC dapat menjadi pendekatan yang tepat untuk memperkuat keamanan data keuangan, khususnya dalam mengendalikan siapa yang dapat mengakses data, fungsi apa yang dapat digunakan, tindakan apa yang dapat dilakukan, dan bagaimana aktivitas tersebut dapat ditelusuri.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada rekan-rekan sejawat yang telah memberikan masukan dan saran konstruktif demi menyempurnakan karya ilmiah ini.

DAFTAR PUSTAKA

Force, J. T. (2020). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology.

Grassi, P., Garcia, M., & Fenton, J. (2020). *Digital identity guidelines*. National Institute of Standards and Technology.

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute based access control (abac) definition and considerations. *NIST Special Publication*, *800*(162), 1–54.

Mercado, I. T., Santos, J. C. S., Matos, L., Gopalakrishnan, R., & Hua, Y. (n.d.). *Detecting OWASP Cheat Sheets in the Source Code*.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0*.

Rakshit, S. K. (2022). *Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks (English Edition)*. BPB Publications.

Rojabi, M. A. (2025). *Pengantar OWASP*. Afdan Rojabi Publisher.