Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No. 4, Tahun 2026
doi.org/10.63822/f98cap10
Hal. 5050-5053

Implementasi Hak Akses User dalam Mencegah Kebocoran Data Jaringan

Intan Sahyuni[1], Aura Chintiya Bella[2], Muhammad Rijal[3], Syaira Ramadhani[4], Eksyel Bongga Upa'[5], Suci Dian Azzahra[6], Ketrin Rinayanti Manullang[7]
Universitas Sulawesi Barat[1-7]

Author's Email: sahyuni1213@gmail.com aurachintiya@gmail.com mrijal4991@gmail.com saira2792007@gmail.com eksyelstel@gmail.com sucimajene82@gmail.com ketrin.rm46@gmail.com

Sejarah Artikel:

Diterima *25-05-2026*
Disetujui *02-06-2026*
Diterbitkan *04-06-2026*

ABSTRACT

Network security has become an important issue in the digital era due to the increasing use of data-based systems in various sectors. Many organizations store important information within computer networks, causing the risk of data leakage to increase significantly. One of the main causes of data leakage is poor user access management. This study aims to analyze the implementation of user access rights in preventing network data leakage through the application of Role-Based Access Control (RBAC) and Network Access Control (NAC). The research method used is a quantitative approach with descriptive-analytical methods and network system simulations. Research data were obtained through user access testing and network activity analysis. The results show that the implementation of RBAC can limit user access according to their duties and responsibilities, thereby reducing the risk of data misuse. In addition, the use of NAC helps the system validate devices that are allowed to access the network. The combination of these two methods has proven effective in improving network security and reducing the risk of data leakage significantly.

Keywords*: user access rights; network security; data leakage; RBAC; NAC*

ABSTRAK

Keamanan jaringan komputer menjadi salah satu hal yang sangat penting di era digital saat ini karena meningkatnya penggunaan sistem berbasis data dalam berbagai bidang. Banyak organisasi menyimpan data penting di dalam jaringan komputer sehingga risiko kebocoran data juga semakin besar. Salah satu penyebab utama kebocoran data adalah pengelolaan hak akses pengguna yang kurang terstruktur. Penelitian ini bertujuan untuk menganalisis implementasi hak akses user dalam mencegah kebocoran data jaringan komputer melalui penerapan Role-Based Access Control (RBAC) dan Network Access Control (NAC). Metode penelitian yang digunakan yaitu pendekatan kuantitatif dengan metode deskriptif analitis serta simulasi sistem jaringan. Data penelitian diperoleh melalui pengujian akses pengguna dan analisis aktivitas sistem jaringan. Hasil penelitian menunjukkan bahwa penerapan RBAC mampu membatasi akses pengguna sesuai tugas dan tanggung jawabnya sehingga risiko penyalahgunaan data dapat dikurangi. Selain itu, penggunaan NAC juga membantu sistem dalam memvalidasi perangkat yang dapat mengakses jaringan. Kombinasi kedua metode tersebut terbukti mampu meningkatkan keamanan jaringan dan mengurangi risiko kebocoran data secara signifikan.

Kata kunci: hak akses user; keamanan jaringan; kebocoran data; RBAC; NAC.

Bagaimana Cara Sitasi Artikel ini:

Sahyuni, I., Bella, A. C. ., Rijal, M. ., Ramadhani, S. ., Upa', E. B., Azzahra, S. D. ., & Rinayanti Manullang, K. (2026). Implementasi Hak Akses User dalam Mencegah Kebocoran Data Jaringan. Jejak Digital: Jurnal Ilmiah Multidisiplin, 2(4), 5050-5053. https://doi.org/10.63822/f98cap10

PENDAHULUAN

Perkembangan teknologi informasi memberikan dampak yang sangat besar terhadap penggunaan sistem jaringan komputer dalam kehidupan sehari-hari. Saat ini hampir semua organisasi, baik di bidang pendidikan, pemerintahan, maupun industri, menggunakan jaringan komputer untuk menyimpan dan mengelola data penting. Data tersebut menjadi aset berharga yang harus dijaga kerahasiaan dan keamanannya agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Seiring meningkatnya penggunaan teknologi digital, ancaman terhadap keamanan data juga semakin meningkat. Salah satu masalah yang sering terjadi adalah kebocoran data, yaitu kondisi ketika informasi penting dapat diakses atau disebarkan oleh pihak yang tidak memiliki hak akses. Kebocoran data dapat terjadi karena serangan dari luar maupun kesalahan dari pengguna internal yang memiliki akses ke sistem.

Dalam banyak kasus, kebocoran data justru terjadi karena pengelolaan hak akses yang kurang tepat. Beberapa pengguna sering kali memiliki akses yang terlalu luas sehingga memungkinkan terjadinya penyalahgunaan data. Selain itu, kurangnya pengawasan terhadap perangkat yang terhubung ke jaringan juga dapat menjadi celah keamanan yang berbahaya.

Untuk mengatasi masalah tersebut, diperlukan sistem pengelolaan akses yang mampu membatasi hak pengguna sesuai kebutuhan pekerjaannya. Salah satu metode yang banyak digunakan adalah Role-Based Access Control (RBAC). Metode ini membagi hak akses berdasarkan peran pengguna sehingga setiap pengguna hanya dapat mengakses data yang berkaitan dengan tugasnya.

Selain RBAC, keamanan jaringan juga dapat ditingkatkan menggunakan Network Access Control (NAC). Sistem ini berfungsi untuk memeriksa perangkat yang ingin terhubung ke jaringan dan memastikan bahwa perangkat tersebut memenuhi standar keamanan yang ditentukan.

Penelitian ini bertujuan untuk menganalisis implementasi hak akses user dalam mencegah kebocoran data jaringan serta mengetahui efektivitas penerapan RBAC dan NAC dalam meningkatkan keamanan sistem jaringan komputer.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode deskriptif analitis. Metode ini digunakan untuk menggambarkan kondisi keamanan jaringan sekaligus menganalisis pengaruh implementasi hak akses terhadap pencegahan kebocoran data.

Penelitian dilakukan melalui simulasi sistem jaringan komputer dengan menerapkan metode Role-Based Access Control (RBAC) dan Network Access Control (NAC). Pada tahap awal dilakukan identifikasi masalah terkait kelemahan sistem keamanan dan pengelolaan hak akses pengguna.

Selanjutnya dilakukan perancangan sistem dengan membagi pengguna ke dalam beberapa kategori, seperti administrator, staf, dan tamu. Setiap kategori diberikan hak akses yang berbeda sesuai kebutuhan operasional masing-masing.

Tahap implementasi dilakukan melalui simulasi berbagai kondisi akses jaringan, seperti akses normal, percobaan akses ilegal, penggunaan perangkat tidak terdaftar, dan pengujian login menggunakan kredensial yang salah.

Data penelitian diperoleh dari log aktivitas sistem jaringan yang mencatat seluruh aktivitas pengguna selama proses pengujian berlangsung. Data tersebut kemudian dianalisis menggunakan metode statistik deskriptif untuk mengetahui hubungan antara penerapan kontrol akses dengan tingkat keamanan jaringan.

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa penerapan sistem kontrol akses berbasis RBAC dan NAC mampu meningkatkan keamanan jaringan secara signifikan. Pengguna hanya dapat mengakses data sesuai dengan hak akses yang diberikan sehingga risiko penyalahgunaan data dapat dikurangi. Selain itu, sistem juga mampu mendeteksi perangkat yang tidak memenuhi standar keamanan sebelum terhubung ke jaringan.

1) Penerapan Role-Based Access Control (RBAC)

Table 1. Pembagian Hak Akses Pengguna

Peran Pengguna	Hak Akses
Administrator	Mengelola seluruh sistem dan data
Staf	Mengakses data sesuai kebutuhan pekerjaan
Tamu	Hanya melihat informasi umum

(Source: Hasil Penelitian, 2026)

Penerapan RBAC membuat pengelolaan akses menjadi lebih terstruktur karena setiap pengguna memperoleh hak akses sesuai perannya. Dengan sistem ini, kemungkinan pengguna mengakses data di luar tanggung jawabnya dapat diminimalkan.

2) Implementasi Network Acsess Control (NAC)

Penerapan NAC membantu sistem dalam memvalidasi perangkat yang akan terhubung ke jaringan. Perangkat yang tidak memenuhi standar keamanan, seperti tidak memiliki antivirus atau menggunakankonfigurasi yang tidak aman, secara otomatis ditolak oleh sistem.

Hasil pengujian menunjukkan bahwa NAC mampu mengurangi risiko ancaman dari perangkat eksternal yang berpotensi membawa malware atau melakukan akses ilegal ke dalam jaringan.

3) Pengaruh Kontrol Akses terhadap Keamanan Jaringan

Berdasarkan hasil analisis, kombinasi RBAC dan NAC memberikan perlindungan yang lebih efektif dibandingkan penggunaan satu metode saja. Sistem keamanan menjadi lebih terkontrol karena akses pengguna dan perangkat dapat diawasi secara bersamaan.

Selain itu, penerapan kontrol akses juga membantu organisasi dalam menerapkan prinsip least privilege, yaitu memberikan hak akses minimum kepada pengguna sesuai kebutuhannya. Dengan pendekatan ini, risiko kebocoran data dapat ditekan secara lebih optimal.

KESIMPULAN

Implementasi hak akses user memiliki peran penting dalam menjaga keamanan jaringan komputer dan mencegah kebocoran data. Berdasarkan hasil penelitian, penerapan Role-Based Access Control (RBAC) mampu membatasi akses pengguna sesuai tugas dan tanggung jawabnya sehingga mengurangi risiko penyalahgunaan data. Selain itu, penggunaan Network Access Control (NAC) membantu meningkatkan keamanan jaringan dengan memvalidasi perangkat yang terhubung ke sistem. Kombinasi kedua metode tersebut terbukti efektif dalam meningkatkan keamanan jaringan dan mengurangi risiko

kebocoran data pada sistem komputer modern.

REFERENSI

Anderson, R. (2020). Security Engineering. Wiley.
Behl, A., & Behl, K. (2017). Cybersecurity and Cyberwar. Springer.
Bishop, M. (2003). Computer Security: Art and Science. Addison-Wesley.
Cisco Systems. (2018). Network Access Control Whitepaper.
ENISA. (2020). Data Protection Guidelines.
Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). Role-Based Access Control. Artech House.
Hu, V. C., Ferraiolo, D., Kuhn, R., et al. (2013). Guide to Attribute Based Access Control (ABAC). NIST.
ISO/IEC 27001:2013. Information Security Management Systems.
Kurose, J. F., & Ross, K. W. (2017). Computer Networking. Pearson.
Sandhu, R., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-Based Access Control Models. IEEE Computer.
Scarfone, K., & Hoffman, P. (2009). NAC Overview. NIST Special Publication.
Stallings, W. (2017). Network Security Essentials. Pearson.
Tanenbaum, A. S. (2011). Computer Networks. Pearson.
Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage.