INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 4 Tahun 2025 Page 1698-1712
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Rancang Bangun Sistem Akses Keamanan Kantor Berbasis RFID dan Biostar 2 Pada Pabrik X

Cahyo Yoga Adhitama[1✉], Yohanes Calvinus[2]
Universitas Tarumanagara
Email: cahyo.525220008@stu.untar.ac.id[1✉]

Abstrak

Keamanan akses di lingkungan kantor merupakan aspek krusial dalam melindungi aset fisik, data, dan dokumen penting perusahaan. Artikel ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan akses pintu berbasis teknologi *Radio Frequency Identification (RFID)* yang terintegrasi dengan perangkat lunak Biostar 2 pada Pabrik X. Sistem ini dirancang untuk menggantikan metode konvensional berbasis kunci mekanis yang rentan terhadap duplikasi dan kelalaian manusia. Perangkat keras utama yang digunakan meliputi *RFID Card Reader Suprema Xpass 2, Magnetic Door Lock, Exit Button, Emergency Breakglass, Power Supply,* dan UPS. Seluruh komponen dirancang secara terintegrasi dan dikelola melalui Biostar 2. Penelitian menggunakan pendekatan *Research and Development (R&D)* dengan tahapan observasi, desain, implementasi, dan pengujian sistem. Hasil pengujian menunjukkan bahwa sistem mampu melakukan autentikasi pengguna secara akurat, mencatat aktivitas akses dalam event log, serta membedakan kartu sah dan tidak sah secara real-time. Nilai kebaruan dari penelitian ini terletak pada penerapan pertama sistem Biostar 2 secara terpusat di lingkungan Pabrik X. Sistem terbukti fleksibel, handal, dan mendukung pengembangan lebih lanjut dalam digitalisasi sistem keamanan fisik industri.

Kata Kunci: *Keamanan Akses, RFID, Biostar 2, Kontrol Pintu, Sistem Keamanan Kantor*

Abstract

Access security in the office environment is a crucial aspect in protecting the company's physical assets, data, and important documents. This article aims to design and implement a door access security system based on Radio Frequency Identification (RFID) technology integrated with Biostar 2 software at Factory X. This system is designed to replace conventional methods based on mechanical keys that are vulnerable to duplication and human error. The main hardware used includes RFID Card Reader Suprema Xpass 2, Magnetic Door Lock, Exit Button, Emergency Breakglass, Power Supply, and UPS. All components are designed in an integrated manner and managed through Biostar 2. The study uses a Research and Development (R&D) approach with stages of observation, design, implementation, and system testing. The test results show that the system is able to authenticate users accurately, record access activities in event logs, and distinguish between valid and invalid cards in real-time. The novelty of this study lies in the first centralized application of the Biostar 2 system in the Factory X environment. The system has proven to be flexible, reliable, and supports further development in the digitalization of industrial physical security systems. Keywords: Access Security, RFID, Biostar 2, Door Control, Office Security System.

Keywords: *Chiller Plant, VAC, Energy Efficiency, Cooling Load, Control Simulation, Energy Saving*

PENDAHULUAN

Keamanan akses dalam lingkungan kantor merupakan aspek penting yang harus diperhatikan dalam melindungi aset fisik, data, dan dokumen penting perusahaan. Kasus yang diberitakan oleh Kompas.com pada 28 Desember 2020 mengungkap sekelompok karyawan yang bersekongkol mencuri barang perusahaan hingga menyebabkan kerugian sebesar Rp 538 juta, yang baru terungkap saat audit dilakukan. Peristiwa ini menegaskan bahwa keamanan akses kantor merupakan hal penting, khususnya untuk mencegah pencurian, kebocoran data, dan akses tidak sah (Ilham et al., 2024). Oleh karena itu, diperlukan desain sistem keamanan pada akses ruangan yang memungkinkan perlindungan optimal serta kemudahan dalam perawatan dan pengembangan komponennya.

Keamanan merupakan aspek vital dalam lingkungan kantor untuk melindungi aset, dokumen, serta memastikan bahwa hanya orang yang berwenang yang dapat mengakses ruangan tertentu. Sebagai elemen utama dalam sistem keamanan, pintu berfungsi sebagai titik keluar-masuk yang harus dikendalikan dengan baik untuk mencegah akses yang tidak sah . Seiring berkembangnya teknologi, sistem keamanan berbasis elektronik telah menjadi solusi yang efektif dalam mengelola akses pintu. Sistem keamanan pintu biasanya masih menggunakan metode mekanis, yang memiliki risiko tinggi terhadap keamanan. Kekurangan sistem ini antara lain mudah diduplikasi dan tidak memiliki pengamanan yang

dapat dikendalikan langsung oleh pemiliknya (Sholehati & Goeritno, 2018). Selain itu, faktor kesalahan manusia seperti keterlambatan dalam membuka kunci juga dapat menyulitkan individu d(Suwanda, 2024)alam keadaan mendesak, atau kelalaian dalam mengunci pintu pada malam hari, yang secara langsung meningkatkan risiko pencurian (Ningrum & Basyir, 2022). Hal-hal tersebut menunjukkan perlunya pengawasan akses yang ketat, khususnya di tempat kerja.

Salah satu solusi yang dapat meningkatkan keamanan akses adalah penerapan teknologi Radio Frequency Identification (RFID), yang memungkinkan proses autentikasi lebih aman dan efisien. Teknologi ini menawarkan keuntungan dalam aspek keamanan karena perangkatnya sulit dipalsukan (Khusnah, 2018). Teknologi Radio Frequency Identification (RFID) merupakan salah satu solusi yang telah banyak diadopsi dalam sistem keamanan modern karena kemudahannya dalam autentikasi pengguna melalui kartu pintar (smart card). Dipadukan dengan perangkat lunak manajemen keamanan seperti Biostar 2, sistem ini tidak hanya mampu mencatat setiap aktivitas akses, tetapi juga memberikan fleksibilitas dalam pengaturan hak akses, pelaporan.

Tujuan dari pemasangan sistem ini di Pabrik X adalah untuk meningkatkan tingkat keamanan ruangan, menggantikan sistem lama yang rawan risiko, serta mengadopsi sistem yang dapat dikembangkan dan dikelola secara efisien. Sistem ini mendukung pengawasan akses berbasis waktu dan lokasi, pencatatan aktivitas secara otomatis, serta kemampuan ekspansi yang memungkinkan kontrol lintas ruangan dalam satu kesatuan sistem. Serta batasan topik difokuskan pada penyusunan sistem keamanan akses, identifikasi komponen yang digunakan, serta penjelasan alur kerja sistem secara umum. Pembahasan tidak mencakup proses implementasi penuh di lingkungan operasional maupun analisis perbandingan dengan sistem keamanan lain yang telah ada. Fokus utama diarahkan pada bagaimana sistem ini dirancang untuk meningkatkan kontrol akses fisik secara efisien, mendukung integrasi dengan sistem tambahan di masa depan, serta mempermudah proses pengelolaan dan pengembangannya.

Penerapan sistem keamanan akses pintu menggunakan BioStar 2 yang terintegrasi dengan berbagai perangkat pendukung ini merupakan inovasi baru di Pabrik X. Sistem sebelumnya bersifat manual dan tidak terpusat, tanpa kemampuan pemantauan real-time. Berbeda dari sistem-sistem sebelumnya atau di perusahaan lain yang masih mengandalkan sistem standalone, sistem ini memperkenalkan transformasi dari sistem konvensional ke sistem keamanan digital yang cerdas, terpusat, dan dapat dikembangkan secara berkelanjutan. Nilai kebaruan dari proyek magang ini terletak pada penerapan pertama

sistem BioStar 2 sebagai pusat kontrol akses terintegrasi di Pabrik X yang mendukung skalabilitas, efisiensi manajemen, dan keamanan yang lebih tinggi di lingkungan kerja.

METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan penelitian dan pengembangan *(Research and Development)* yang bertujuan untuk merancang dan menghasilkan sebuah sistem keamanan akses pintu yang terintegrasi dan dapat diterapkan secara langsung di lingkungan kantor berdasarkan hasil uji coba lapangan dan masukan dari pengguna, metode R&D tidak hanya berhenti pada penciptaan produk, tetapi juga melibatkan proses validasi, evaluasi, serta perbaikan produk [6]. Metode ini dipilih karena mampu menjawab kebutuhan nyata di lapangan, sebagaimana diungkapkan dalam kasus pencurian aset perusahaan yang terjadi akibat lemahnya sistem keamanan dan kontrol akses.

Metode ini juga melibatkan pengamatan langsung di lapangan untuk memahami situasi dan kebutuhan sistem keamanan secara riil. Pengamatan dilakukan untuk mengidentifikasi potensi celah keamanan serta menilai efektivitas sistem yang dirancang berdasarkan kondisi sebenarnya di lingkungan kerja. Melalui pendekatan ini, penelitian dilakukan secara sistematis dimulai dari identifikasi masalah di lingkungan kerja, analisis kebutuhan sistem keamanan, hingga perancangan dan pengujian sistem yang melibatkan komponen seperti card reader RFID, magnetic lock, emergency breakglass, exit button, power supply, UPS, dan kabel UTP CAT 6. Selain itu, penggunaan perangkat lunak Biostar 2 memungkinkan pengelolaan akses yang lebih terpusat dan fleksibel. Dengan demikian, metode ini memungkinkan pengembangan sistem yang tidak hanya efektif dari segi keamanan, tetapi juga efisien dalam hal pemeliharaan dan siap untuk dikembangkan lebih lanjut di masa depan.

Analisis Kebutuhan Sistem

Metode penelitian ini menggunakan pendekatan penelitian dan pengembangan (Research and Development) yang bertujuan untuk merancang dan menghasilkan sebuah sistem keamanan akses pintu yang terintegrasi dan dapat diterapkan secara langsung di lingkungan kantor berdasarkan hasil uji coba lapangan dan masukan dari pengguna, metode R&D tidak hanya berhenti pada penciptaan produk, tetapi juga melibatkan proses validasi, evaluasi, serta perbaikan produk [6]. Metode ini dipilih karena mampu menjawab kebutuhan nyata di lapangan, sebagaimana diungkapkan dalam kasus pencurian aset perusahaan yang terjadi akibat lemahnya sistem keamanan dan kontrol akses.

Metode ini juga melibatkan pengamatan langsung di lapangan untuk memahami situasi dan kebutuhan sistem keamanan secara riil. Pengamatan dilakukan untuk mengidentifikasi potensi celah keamanan serta menilai efektivitas sistem yang dirancang berdasarkan kondisi sebenarnya di lingkungan kerja. Melalui pendekatan ini, penelitian dilakukan secara sistematis dimulai dari identifikasi masalah di lingkungan kerja, analisis kebutuhan sistem keamanan, hingga perancangan dan pengujian sistem yang melibatkan komponen seperti card reader RFID, magnetic lock, emergency breakglass, exit button, power supply, UPS, dan kabel UTP CAT 6. Selain itu, penggunaan perangkat lunak Biostar 2 memungkinkan pengelolaan akses yang lebih terpusat dan fleksibel. Dengan demikian, metode ini memungkinkan pengembangan sistem yang tidak hanya efektif dari segi keamanan, tetapi juga efisien dalam hal pemeliharaan dan siap untuk dikembangkan lebih lanjut di masa depan.

1. Kebutuhan Fungsional

Kebutuhan fungsional menggambarkan fungsi – fungsi utama yang harus dimiliki oleh sistem, antara lain:

Tabel 1. Kebutuhan Fungsional

No	Kebutuhan Fungsional	Keterangan
1.	Pengelolaan hak akses pengguna	Sistem harus dapat membedakan akses antara karyawan, tamu, dan admin
2.	Registrasi dan sinkronisasi RFID card	RFID card harus dapat didaftarkan ke dalam sistem Biostar 2
3.	Autentikasi dan pengendalian pintu masuk/keluar	Pintu hanya terbuka untuk pengguna yang memiliki izin
4.	Logging aktivitas akses pengguna	Setiap aktivitas tersimpan kedalam database sistem
5.	Mekanisme darurat	Tersedia tombol darurat (emergency breakglass) untuk membuka pintu manual
6.	Kontrol akses real-time melalui software	Akses pintu dapat dikontrol dan dimonitor secara langsung melalui Biostar 2
7.	Fungsi tombol keluar (Exit Button)	Pintu dapat dibuka dari dalam ruangan tanpa kartu dengan tombol sentuh

2. Kebutuhan Non Fungsional

Kebutuhan non-fungsional berkaitan dengan kualitas sistem dan aspek pendukung lainnya, seperti:

Tabel 2. Kebutuhan Non Fungsional

No	Kebutuhan Non Fungsional	Keterangan
1.	Keamanan data	Data akses harus terenkripsi dan hanya dapat diakses oleh admin
2.	Redundasi daya	Sistem harus tetap aktif saat listrik padam dengan bantuan UPS
3.	Skalabilitas dan fleksibilitas	Sistem harus dapat dikembangkan untuk pintu dan pengguna tambahan
4.	Kemudahan perawatan dan instalasi	Setiap aktivitas tersimpan kedalam database sistem
5.	Mekanisme darurat	Perangkat mudah dipasang dan dirawat
6.	Kemudahan menggunakan sistem	Penggunaan Biostar 2 harus mudah dipahami oleh operator/admin teknis

Kebutuhan Komponen Sistem

Sistem keamanan akses yang diterapkan di Pabrik X terdiri dari berbagai komponen utama yang saling terintegrasi mencakup perangkat keras dan perangkat lunak yang bekerja secara sinergis. Pada sisi perangkat lunak, digunakan Biostar 2, sebuah sistem manajemen akses yang mampu membentuk jaringan mandiri melalui pengaturan alamat IP perangkat serta berfungsi sebagai pusat kendali untuk konfigurasi hak akses, pengelolaan event log real-time, dan pengaturan pengguna berdasarkan departemen atau fungsi tertentu. Biostar 2 ini diinstal pada server utama dan menjadi pengendali penuh dari seluruh sistem yang beroperasi.

Komponen perangkat kerasnya mencakup Radio Frequency Identification (RFID) Card Reader Suprema Xpass 2 yang menggunakan teknologi RFID untuk membaca chip unik pada kartu pengguna secara nirkabel melalui gelombang radio (Abugabah et al., 2020). Saat kartu ditempelkan, sistem akan mencocokkan ID dengan database Biostar dan memberikan akses hanya kepada kartu yang terdaftar secara sah. Akses fisik ke ruangan dikendalikan oleh Magnetic Door Lock, yaitu kunci elektromagnetik yang menahan pintu tetap tertutup hingga sistem memberikan otorisasi berdasarkan hasil autentikasi (Hashim et al., 2023). Dari sisi dalam, pintu dapat dibuka menggunakan Exit Button berbasis sensor sentuh, yang memberikan kemudahan operasional tanpa memerlukan kartu akses.

Untuk kondisi darurat seperti kebakaran atau evakuasi mendesak, tersedia Emergency Breakglass yang memungkinkan pembukaan pintu secara manual hanya dalam keadaan darurat dengan memecahkan atau menekan kaca pengaman (Belguith et al., 2018). Semua

perangkat ini mendapatkan daya dari Power Supply 12V MEAN WELL AD 155A yang mengubah arus AC menjadi DC sesuai kebutuhan masing-masing perangkat (Muhammad et al., 2021), serta didukung oleh Uninterruptible Power Supply (UPS) sebagai sumber daya cadangan yang secara otomatis aktif saat terjadi pemadaman (Lubis et al., 2022).

Untuk menjamin komunikasi data antar perangkat, digunakan Switch jaringan yang efisien karena hanya mengarahkan data ke port tujuan, bukan menyebarkannya ke semua perangkat, sehingga stabilitas komunikasi sistem dapat terjaga (Pranata & Harahap, 2024). Komponen-komponen ini terhubung melalui Kabel UTP CAT 6, yang mampu mentransmisikan data dengan kecepatan tinggi hingga 10 Gbps (Santoso et al., 2023), serta Kabel NYAF yang digunakan dalam distribusi daya antar perangkat berkat fleksibilitas dan keandalannya dalam instalasi panel listrik (Saleh Muhamad & Haryanti Munnik, 2017).

Dengan konfigurasi sistem yang menyeluruh dan terintegrasi ini sistem keamanan akses di Pabrik X dirancang tidak hanya untuk menjamin keamanan, tetapi juga untuk memastikan efisiensi operasional serta kesiapan menghadapi kondisi darurat atau gangguan teknis.

Perbandingan Sistem Keamanan Akses Konvensional dan Elektronik

Sistem keamanan akses secara umum dapat dibedakan menjadi dua kategori, yaitu sistem konvensional dan sistem elektronik. Sistem konvensional umumnya menggunakan kunci mekanis, sementara sistem elektronik mengandalkan perangkat otomatis seperti RFID, biometrik, atau PIN. Sistem konvensional memiliki keunggulan dalam hal biaya awal yang rendah dan kemudahan dalam implementasi. Namun, sistem ini memiliki keterbatasan signifikan, seperti:

- Rentan terhadap duplikasi kunci fisik,
- Tidak adanya pencatatan aktivitas akses, dan
- Tidak dapat dikendalikan secara terpusat.

Sebaliknya, sistem elektronik berbasis RFID memungkinkan autentikasi otomatis, pengelolaan hak akses berbasis perangkat lunak, serta pencatatan seluruh aktivitas pengguna dalam bentuk *event log*. Hal ini membuatnya lebih efektif dalam konteks keamanan yang menuntut keandalan tinggi dan fleksibilitas pengelolaan. Penerapan teknologi RFID juga meminimalisir risiko kesalahan manusia seperti kehilangan kunci atau kelalaian dalam mengunci pintu. Dalam penelitian ini, sistem RFID yang diintegrasikan dengan software Biostar 2 dirancang sebagai solusi terhadap kelemahan-kelemahan tersebut.

Keunggulan Sistem RFID Berbasis Biostar 2 dibanding Sistem Lain

Biostar 2 adalah perangkat lunak manajemen akses yang dikembangkan oleh Suprema dan dirancang untuk integrasi dengan perangkat kontrol akses seperti RFID reader, biometric reader, dan CCTV. Dibandingkan dengan software kontrol akses lain seperti ZKTeco, HID, atau sistem open-source berbasis Arduino, Biostar 2 menawarkan keunggulan sebagai berikut:

Tabel 3. Perbandingan Biostar 2 dengan sistem lain

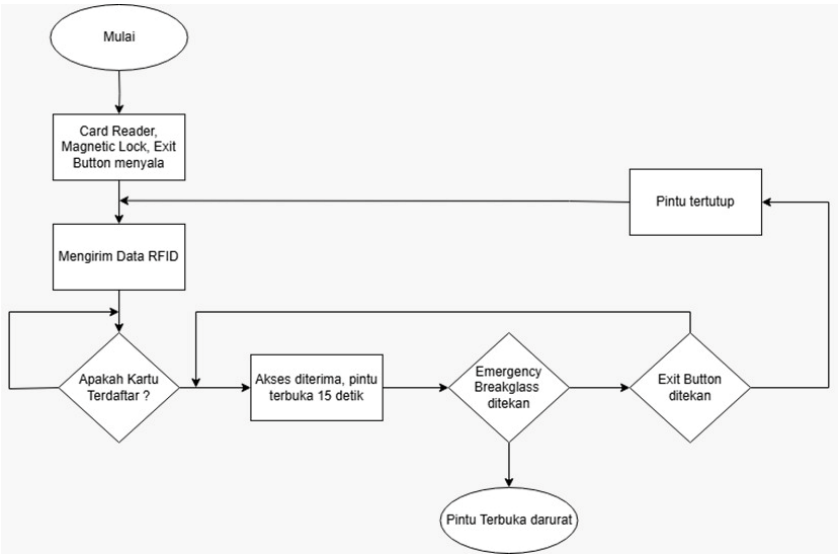
Fitur	Biostar 2	Sistem Lain (umum)
Berbasis Web	Ya	Tidak semua
Event Log Real-Time	Ya	Terbatas / Tidak ada
Hak Akses Per User & Departemen	Ya	Terbatas
Dukungan Multi Reader	Ya	Biasanya hanya 1-2 reader
Integrasi dengan Emergency System	Ya	Tidak semua
Enkripsi dan Keamanan Data	Ya (TLS & DB Secure)	Tidak tersedia di semua sistem

Keunggulan itu menjadikan Biostar 2 cocok untuk kebutuhan industri seperti Pabrik X, yang menuntut tingkat keamanan tinggi dan kemampuan pengelolaan akses yang fleksibel. Selain itu sistem ini juga mendukung pengembangan serta pemeliharaan yang efisien, karena konfigurasi dapat dilakukan melalui web. Dengan ini Biostar 2 menawarkan efisiensi, keamanan, dan kemudahan administrasi yang unggul dibandingkan software kontrol akses sekelasnya.

HASIL DAN PEMBAHASAN

Tahapan yang diperlukan dalam membuat pengembangan dan pembaruan dalam sebuah sistem dapat dilakukan dengan melihat sistem yang telah ada, dimana analisa ini merupakan suatu proses untuk mempelajari sistem dengan cara menguraikan sistem tersebut.

Diagram Blok



Gambar 1 Diagram Blok

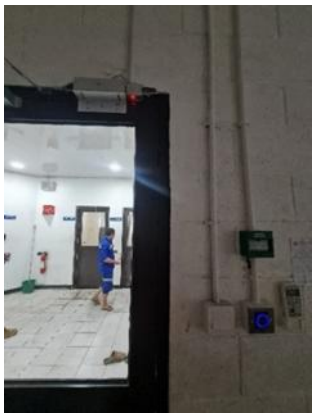
Perangkat Keras Sistem Keamanan

Perangkat keras desain sistem keamanan akses ruangan kantor pada pabrik x

1. *Door Magnetic Lock*
2. *RFID Card Reader*
3. *Exit Button*
4. *Power Supply*
5. *Uninterruptible Power Supply*
6. Kabel UTP CAT 6
7. Kabel NYAF

Perangkat keras desain sistem keamanan akses ruangan kantor pada pabrik x dapat dilihat pada gambar dibawah:

Gambar 2. Tampak Luar

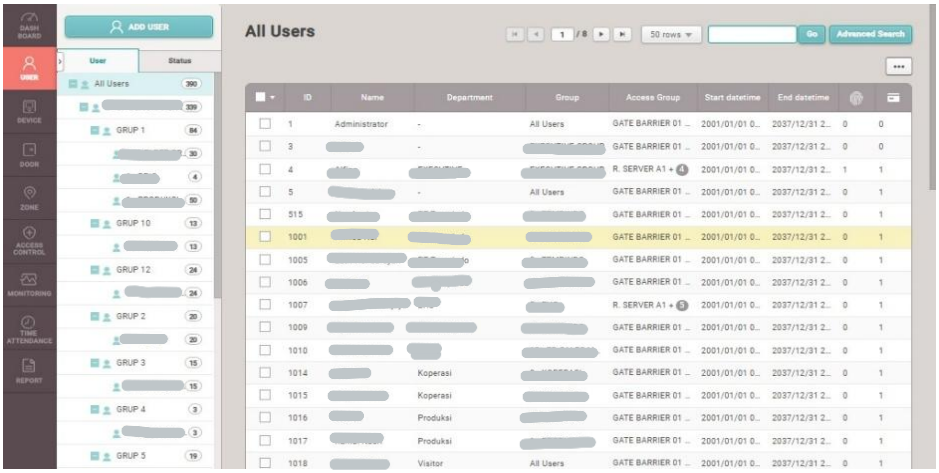


Gambar 3. Tampak Dalam

Gambar 4. Panel *Power Supply*

Perangkat Lunak Sistem Keamanan

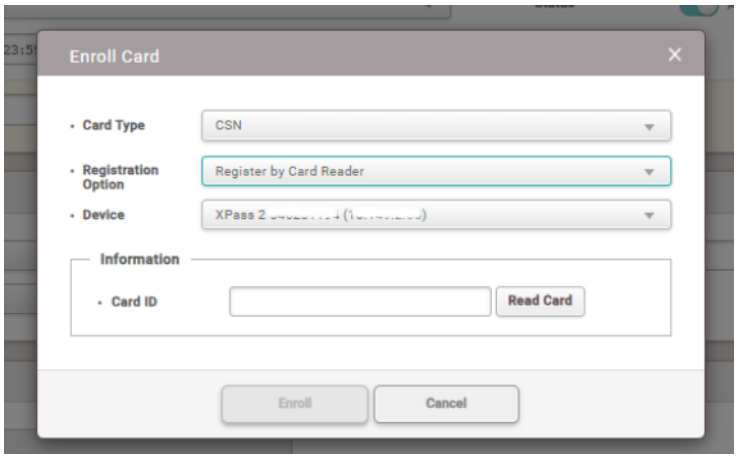
Software yang digunakan pada sistem kali ini merupakan software Biostar 2 yang berfungsi untuk pengaturan hak akses kartu, pengelompokan pengguna berdasarkan departemen atau fungsi, serta penambahan user ke dalam sistem. Dibawah ini akan menunjukkan dimana sistem dari perangkat keras terhubung kedalam perangkat lunak.



Gambar 5. Daftar User

Proses Penambahan Kartu

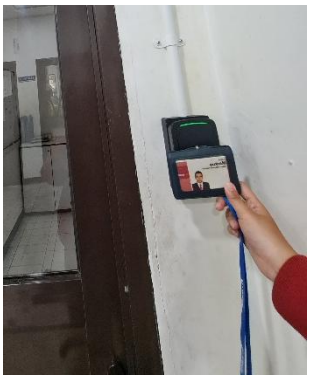
Proses penambahan kartu dilakukan untuk mendaftarkan identitas pengguna ke dalam sistem keamanan sehingga dapat diberikan hak akses sesuai kebutuhan. Langkah ini dilakukan melalui perangkat lunak Biostar 2 dengan menghubungkan kartu RFID ke card reader dan memasukkan data pengguna seperti nama, departemen, dan hak akses ruangan. Setelah data pengguna dan kartu berhasil direkam, kartu tersebut akan tersimpan dalam database sistem dan dapat digunakan untuk mengakses pintu yang telah ditentukan. Proses ini memastikan bahwa hanya pengguna yang telah terdaftar dan terverifikasi yang dapat mengakses area tertentu di lingkungan kantor.



Gambar 6. Proses Pendaftaran Kartu

Pengujian Kartu Terdaftar

Pengujian ini dilakukan untuk memastikan bahwa sistem dapat mengenali dan memberikan akses kepada kartu yang telah terdaftar sebelumnya. Pengguna menempelkan (tap) kartu yang sudah didaftarkan ke perangkat RFID Card Reader. Sistem kemudian membaca data kartu dan mencocokkannya dengan database yang ada di software Biostar 2. Hasil pengujian menunjukkan bahwa kartu berhasil dikenali oleh sistem dan ditampilkan dalam event log sebagai aktivitas autentikasi yang berhasil. Setelah proses autentikasi selesai, sistem secara otomatis mengaktifkan Magnetic Lock sehingga pintu terbuka. Hal ini membuktikan bahwa proses pengenalan kartu dan pemberian hak akses berjalan sesuai dengan yang diharapkan.



Gambar 7. Proses tap kartu terdaftar

544288967	Bio[redacted]544288967 (192[redacted]			Door locked
544288967	Bi[redacted]544288967 (192[redacted]			Door unlocked
544288967	Bio[redacted]544288967 (192[redacted]	RUANG NALIN R	14(NALIN (1)[redacted]	1:1[redacted]lication succeeded (Card)
544288967	Bi[redacted]544288967 (192[redacted]			Door locked
544288967	Bio[redacted]544288967 (192[redacted]			Door unlocked
544288967	Bio[redacted]544288967 (192[redacted]	RUANG NALIN R	15(NALIN (2)[redacted]	1:1[redacted]cation succeeded (Card)
544288967	Bi[redacted]544288967 (192[redacted]			Door locked

Gambar 8. Tampilan event log saat kartu terdaftar

Tabel 4. Pengujian tap kartu

Percobaan 1	Akses Berhasil
Percobaan 2	Akses Berhasil
Percobaan 3	Akses Berhasil

Tabel di atas menyajikan hasil uji coba penggunaan kartu. Ketiga percobaan menunjukkan bahwa kartu berhasil terdaftar dan mampu mengakses sistem secara optimal.

Pengujian Kartu Tidak Terdaftar

Pengujian ini dilakukan untuk memastikan bahwa sistem dapat membedakan antara kartu yang telah terdaftar dan kartu yang tidak memiliki izin akses. Dalam pengujian ini, kartu yang belum terdaftar dalam sistem Biostar 2 dicoba untuk digunakan pada RFID Card Reader. Hasilnya, sistem berhasil mendeteksi bahwa kartu tersebut tidak dikenali dan secara otomatis menolak akses. Hal ini ditampilkan secara real-time pada antarmuka perangkat lunak Biostar 2 melalui tampilan event log, yang menunjukkan bahwa percobaan akses ditolak karena kartu tidak valid. Dengan demikian, sistem terbukti mampu menjalankan fungsi autentikasi dengan baik, termasuk dalam menolak akses yang tidak sah.

Gambar 9. Proses tap kartu tidak terdaftar

Gambar 10. Tampilan event log saat kartu tidak terdaftar

Tabel 5. Pengujian tap kartu

Percobaan 1	Akses Ditolak
Percobaan 2	Akses Ditolak
Percobaan 3	Akses Ditolak

Tabel di atas menunjukkan hasil pengujian tap kartu untuk kartu yang tidak terdaftar. Berdasarkan hasil pengujian tersebut, kartu tidak memiliki akses untuk membuka ruangan.

SIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem keamanan akses ruangan kantor berbasis RFID dan Biostar 2 pada Pabrik X, dapat disimpulkan bahwa sistem ini mampu meningkatkan tingkat keamanan secara signifikan dibandingkan metode konvensional yang masih menggunakan kunci mekanis. Sistem yang dibangun memungkinkan proses autentikasi pengguna dilakukan secara otomatis dan terpusat melalui software Biostar 2, yang mampu mencatat setiap aktivitas akses dalam bentuk event log. Perangkat keras seperti *RFID Card Reader, Magnetic Lock, Exit Button, Emergency Breakglass,* serta sistem daya cadangan (UPS) bekerja secara terintegrasi untuk memberikan kontrol akses yang aman dan efisien. Hasil pengujian menunjukkan bahwa sistem dapat membedakan antara kartu yang terdaftar dan tidak terdaftar dengan respon yang tepat, serta dapat diatur sesuai hak akses masing-masing pengguna. Secara keseluruhan, sistem ini memberikan solusi keamanan yang fleksibel, mudah dikelola, dan

siap dikembangkan lebih lanjut untuk mendukung transformasi digital sistem keamanan fisik di lingkungan industri.

Sebagai tindak lanjut dari implementasi sistem ini, disarankan untuk melakukan pemeliharaan rutin terhadap seluruh perangkat keras yang digunakan, seperti *RFID Reader, Magnetic Lock, Exit Button, dan Power Supply*, untuk memastikan sistem tetap berfungsi dengan optimal. Selain itu, penting untuk melakukan pengecekan secara berkala terhadap setiap komponen sistem, agar potensi kerusakan atau gangguan teknis dapat dideteksi dan ditangani lebih awal. Pelatihan teknis bagi operator sistem juga perlu diberikan agar pengelolaan dan konfigurasi sistem dapat dilakukan dengan benar dan efisien. Dengan penerapan saran-saran ini, diharapkan sistem keamanan akses dapat terus berjalan secara andal dan mendukung aktivitas operasional kantor dengan aman.

DAFTAR PUSTAKA

Abugabah, A., Nizamuddin, N., & Abuqabbeh, A. (2020). A review of challenges and barriers implementing RFID technology in the Healthcare sector. Procedia Computer Science, 170, 1003–1010. https://doi.org/10.1016/j.procs.2020.03.094

Belguith, S., Gochhayat, S. P., Conti, M., & Russello, G. (2018). Emergency Access Control Management Via Attribute Based Encrypted QR Codes. 2018 IEEE Conference on Communications and Network Security (CNS), 1–8. https://doi.org/10.1109/CNS.2018.8433186

Hashim, K. A., Qasim, H. H., Hamzah, A. E., Hasan, O. A., & Al-Jadiri, M. (2023). Door lock system based on internet of things and Bluetooth by using Raspberry Pi. Bulletin of Electrical Engineering and Informatics, 12(5), 2753–2762. https://doi.org/10.11591/eei.v12i5.5134

Ilham, A., Mashudi, A., & Prihanto, A. (2024). Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication. 06, 630–638.

Khusnah, A. (2018). Use of Radio Frequency Identification (RFID) System in Supporting Borrowing at Sidoarjo Regency Library and Archives Agency. Jurnal Pendidikan Administrasi Perkantoran (JPAP), 6(2), 169–173. https://ejournal.unesa.ac.id/index.php/JPAPUNESA/article/view/32144

Lubis, R. S., Haris, A., & Tarmizi, T. (2022). UPS Design for Increased Flexibility of Use and More Economic with PWM Controlled Inverter Based on ATmega 328 Microcontroller. Teknik, 43(1), 102–111. https://doi.org/10.14710/teknik.v43i1.32736

Muhammad, U., Mukhlisin, Nuardi, Mansur, A., & Aditya Bachri Maulana, M. (2021).

Rancang Bangun Power Supply Adjustable Current pada Sistem Pendingin Berbasis Termoelektrik. Journal Of Electrical Engginering (Joule), 2(2), 106–110.

Ningrum, N. K., & Basyir, A. (2022). PERANCANGAN SISTEM KEAMANAN PINTU RUANGAN OTOMATIS MENGGUNAKAN RFID BERBASIS INTERNET OF THINGS (IoT). Jurnal Ilmiah Matrik, 24(1), 21–27. https://doi.org/10.33557/jurnalmatrik.v24i1.1651

Pranata, A., & Harahap, R. R. (2024). PERANCANGAN SISTEM JARINGAN MENGGUNAKAN SWITCH CISCO PADA PT . PRIMA INDONESIA LOGISTIK. 4307(August), 855–860.

Saleh Muhamad, & Haryanti Munnik. (2017). Rancang Bangun Sistem Keamanan Rumah Menggunakan Relay. Jurnal Teknologi Elektro, Universitas Mercu Buana, 8(2), 87–94.

Santoso, A. A., Wara, F. A., & Reja, I. D. (2023). Analisa Jaringan Komputer Pada Studio Foto Varia Indah Menggunakan Metode Quality of Services (QoS). Jurnal In Create (Inovasi Dan Kreasi Dalam Teknologi Informasi, 9(1), 53–65.

Sholehati, M. T., & Goeritno, A. (2018). Sistem Minimum Berbasis Mikrokontroler ATmega2560 sebagai Sistem Pengaman pada Analogi Lemari Penyimpanan Brankas. Jurnal Rekayasa Elektrika, 14(3). https://doi.org/10.17529/jre.v14i3.11649

Suwanda, I. (2024). Rancang Bangun Sepeda Listrik Self Charging Dengan Memanfaatkan Motor Dc Sebagai Alternator. 03(01), 7–12. https://doi.org/10.58466/entries.