KAINAN: Jurnal Pengabdian Teknik Informatika
Vol. 1 No. 1, xxxxxx xxx (xxx-xxx) https://doi.org/10.23960/kainan

IMPLEMENTASI MANAJEMEN HAK AKSES DAN KEAMANAN SISTEM ARSIP DIGITAL MENGGUNAKAN NEXTCLOUD PADA BBWS MESUJI SEKAMPUNG

(*Implementation of Access Rights Management and Security of Digital Archive System Using Nextcloud At Bbws Mesuji Sekampung*)

Raffi Rizki Nugraha[1*], Gigih Forda Nama[1], Rio Ariestia Pradipta[1], Farisan Haidi[2]

[1]*Program Studi Teknik Informatika, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Bandar Lampung 35145, Indonesia*
[2] *Balai Besar Wilayah Sungai Mesuji Sekampung, Jl. Gatot Subroto No. 57, Bandar Lampung 35401, Indonesia*

**** Email Korespondensi:***

2215061108@students.unila.ac.id

Abstrak: Pengelolaan arsip digital pada instansi pemerintah memerlukan standar keamanan dan pengaturan akses yang memadai demi menjaga integritas data. Saat ini, penyimpanan dokumen di BBWS Mesuji Sekampung masih menggunakan media fisik dan penyimpanan awan pribadi yang berisiko terhadap keamanan serta menyulitkan kontrol akses. Kegiatan ini bertujuan mengimplementasikan sistem arsip digital berbasis Nextcloud dengan manajemen pengguna dan keamanan data. Metode pengembangan meliputi penerapan Role-Based Access Control (RBAC) untuk izin akses folder, Cloudflare Tunnel untuk enkripsi jalur publik, serta Multi-Factor Authentication (MFA) untuk keamanan administrator. Hasil implementasi menunjukkan sistem mampu membatasi akses dokumen lintas bidang secara efektif dan menjamin keamanan koneksi, serta meminimalisir risiko akses tidak sah. Sistem ini diharapkan mewujudkan pengelolaan arsip yang lebih terstruktur, aman, dan efisien bagi operasional instansi.

Kata kunci: arsip digital, cloudflare tunnel, keamanan informasi, nextcloud, role-based access control

Abstract: *Government agency digital archive management requires adequate security standards and access settings to maintain data integrity. Currently, document storage at BBWS Mesuji Sekampung still uses physical media and private cloud storage, which poses security risks and makes access control difficult. This activity aims to implement a Nextcloud-based digital archive system with user management and data security. Development methods include the application of Role-Based Access Control (RBAC) for folder access permissions, Cloudflare Tunnel for public path encryption, and Multi-Factor Authentication (MFA) for administrator security. The implementation results show that the system can effectively restrict cross-sectoral document access and ensure connection security, as well as minimize the risk of unauthorized access. This system is expected to realize a more structured, secure, and efficient archive management for agency operations.*

Keywords: *cloudflare tunnel, digital archive, information security, nextcloud, role-based access control*

1. PENDAHULUAN

Balai Besar Wilayah Sungai (BBWS) Mesuji Sekampung merupakan instansi yang mengelola dokumen teknis dan operasional dalam jumlah besar lintas bidang. Hingga saat ini, pengelolaan arsip di lingkungan tersebut masih didominasi oleh penggunaan media penyimpanan fisik seperti *flashdisk* dan *harddisk* eksternal, serta layanan penyimpanan awan pribadi yang tidak terintegrasi. Pola penyimpanan tersebut menimbulkan berbagai risiko, antara lain potensi kehilangan data akibat kerusakan perangkat, duplikasi berkas yang tidak terkontrol, serta kesulitan dalam proses pencarian dokumen secara cepat dan efisien. Selain itu, ketiadaan mekanisme kontrol akses yang terpusat membuka celah keamanan, karena tidak terdapat batasan yang jelas mengenai pihak yang berwenang untuk membaca maupun memodifikasi dokumen tertentu.

Permasalahan fragmentasi data tersebut menuntut solusi penyimpanan yang tersentralisasi namun tetap mampu menjaga integritas dan kerahasiaan informasi. Implementasi private cloud storage menjadi alternatif yang relevan bagi instansi pemerintah karena memungkinkan pengelolaan data secara mandiri dalam infrastruktur yang

sepenuhnya berada di bawah kendali organisasi. Salah satu platform yang mendukung pendekatan ini adalah Nextcloud, sebuah sistem *open-source* yang menyediakan fleksibilitas dalam manajemen pengguna dan pengaturan hak akses. *Fitur Role-Based Access Control* yang tersedia pada platform ini memungkinkan pemberian kewenangan berdasarkan peran dan tanggung jawab pengguna, sehingga risiko akses tidak sah dapat diminimalkan.

Di sisi lain, aspek keamanan jaringan menjadi semakin krusial ketika layanan internal diakses melalui jaringan publik. Penggunaan protokol HTTPS dengan enkripsi *Transport Layer Security* (TLS) dan pemanfaatan Cloudflare Tunnel diterapkan untuk melindungi transmisi data dari ancaman penyadapan dan serangan tanpa perlu mengekspos server secara langsung ke internet. Selain perlindungan pada jalur komunikasi, penguatan autentikasi juga diperlukan untuk mencegah penyalahgunaan kredensial. Mekanisme *Multi-Factor Authentication* (MFA) berbasis *Time-Based One-Time Password* (TOTP) memberikan lapisan verifikasi tambahan yang bersifat dinamis, sehingga akses sistem tidak hanya bergantung pada satu faktor autentikasi konvensional.

Beberapa penelitian terdahulu telah mengeksplorasi pemanfaatan komputasi awan dan keamanan jaringan secara terpisah. Pada aspek infrastruktur penyimpanan, Herdiansyah dan Novendra [1] serta Irawan dkk. [2] membuktikan bahwa implementasi *Network Attached Storage* (NAS) berbasis TrueNAS dan Nextcloud sangat efektif dalam memodernisasi tata kelola arsip fisik menjadi digital yang terpusat di instansi pemerintahan maupun pendidikan. Namun, penelitian tersebut belum mengintegrasikan skema pembatasan hak akses yang komprehensif. Terkait kontrol akses, Rubiyanto dkk. [3] dan Sahyudi & Susanto [4] menegaskan bahwa penerapan RBAC dengan prinsip *least privilege* sangat krusial untuk mencegah akses ilegal pada data berskala enterprise dan pemerintahan.

Sementara itu, pada aspek keamanan, Bahalwan dan Febriawan [5] menyoroti urgensi penggunaan Cloudflare Tunnel sebagai jembatan terenkripsi yang menyembunyikan identitas IP asli server tanpa perlu membuka *port* publik. Pengamanan ini semakin esensial jika dipadukan dengan autentikasi berlapis. Fitriyansyah dan Hazri [6] membuktikan bahwa penambahan lapisan TOTP secara signifikan mempersempit celah penyusupan akibat kebocoran kredensial. Merujuk pada pemisahan fokus dari berbagai penelitian tersebut, masih jarang ditemukan studi yang memadukan seluruh entitas teknologi ini secara bersamaan.

Berdasarkan kondisi dan celah kegiatan tersebut, proyek ini menawarkan pembaruan untuk merancang dan mengimplementasikan ekosistem keamanan terpadu pada sistem arsip digital berbasis Nextcloud di BBWS Mesuji Sekampung. Fokus pengembangan meliputi penyatuan manajemen hak akses RBAC, penyediaan jalur komunikasi publik yang aman melalui Cloudflare Tunnel, penguatan autentikasi administratif menggunakan MFA, hingga otomasi pemulihan kredensial via SMTP. Implementasi ini diharapkan mampu meningkatkan efisiensi pengelolaan dokumen sekaligus memperkuat postur keamanan data digital di lingkungan instansi secara berkelanjutan.

2. BAHAN DAN METODE PENELITIAN

Bagian ini menguraikan spesifikasi alat dan bahan pendukung serta tahapan metode yang digunakan dalam perancangan keamanan akses layanan arsip digital di BBWS Mesuji Sekampung. Implementasi ini menggunakan pendekatan pengembangan infrastruktur private cloud dengan mengedepankan isolasi server dari akses jaringan internet secara langsung.

2.1 Metodologi

Untuk memastikan arsitektur yang dibangun berjalan secara sistematis dan terukur, pengembangan sistem dilakukan melalui empat tahapan utama, yaitu:

1. Analisis Kebutuhan: Tahap awal berupa identifikasi permasalahan pada sistem penyimpanan arsip. Hasil observasi menunjukkan pengelolaan dokumen kerja di BBWS Mesuji Sekampung masih mengandalkan media fisik yang memicu fragmentasi data dan tidak adanya mekanisme kontrol akses.
2. Perancangan Sistem: Tahap penyusunan arsitektur untuk memisahkan jalur akses pengguna dan administrator, serta perumusan matriks pembatasan akses.
3. Implementasi Sistem: Tahap penerapan konfigurasi keamanan dan manajemen hak akses pada layanan arsip digital Nextcloud yang telah berjalan di server instansi. Fokus pengerjaan meliputi pengamanan jalur komunikasi publik menggunakan integrasi Cloudflare Tunnel dan enkripsi SSL/TLS, pembatasan otorisasi direktori melalui *Role-Based Access Control*, penguatan keamanan login akun administrator dengan *Multi-Factor Authentication* (MFA), serta integrasi layanan *Simple Mail Transfer Protocol* eksternal untuk otomasi pemulihan kata sandi.
4. Pengujian Sistem: Tahap evaluasi akhir untuk memvalidasi fungsionalitas dan keamanan koneksi, otorisasi folder, autentikasi, dan fitur pemulihan akun.

2.2 Alat dan Bahan

Pengembangan sistem ini memanfaatkan kombinasi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang dirancang khusus

untuk mendukung infrastruktur penyimpanan terpusat berbasis *Network Attached Storage* (NAS) dan keamanan akses. Integrasi antar komponen ini mampu mengubah tata kelola data yang awalnya tersebar secara lokal menjadi lebih terstruktur di dalam satu lingkungan yang terkontrol.

Pemilihan TrueNAS SCALE didasari oleh arsitekturnya yang berbasis Linux Debian. Sistem ini sangat mendukung kemudahan virtualisasi aplikasi, sehingga Nextcloud bisa berjalan langsung secara *native*. Daftar lengkap perangkat lunak dan spesifikasi server yang digunakan dalam implementasi ini disajikan pada Tabel 1 dan Tabel 2.

Tabel 1. Alat dan Bahan

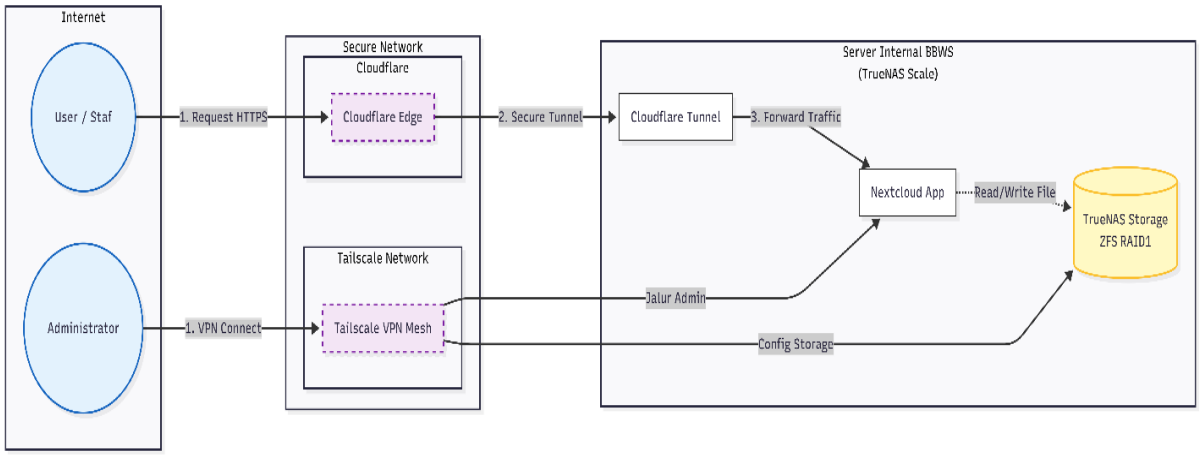
No	Nama	Versi	Keterangan
1	Server Rainer STOR DSX-MT	-	Server utama sistem
2	TrueNAS SCALE	25.04.2.5	Sistem operasi NAS
3	Nextcloud	32.0.1	Sistem arsip digital
4	Cloudflare	-	DNS dan keamanan akses
5	Cloudflared	1.3.24	Cloudflare Tunnel client
6	Brevo SMTP	-	Email notifikasi

Tabel 2. Spesifikasi Server

No	Komponen	Spesifikasi
1	Prosesor	Intel(R) Celeron(R) N5105 @ 2.00GHz
2	RAM	32 GB
3	Media Penyimpanan	*Harddisk* 2 x 8 TB
4	Jaringan	*Ethernet* (LAN)

2.3 Arsitektur Sistem

Sistem dirancang dengan menempatkan Nextcloud sebagai lapisan aplikasi utama dan TrueNAS sebagai media penyimpanan *backend*. Perancangan ini memisahkan alur akses antara pengguna staf dan administrator. Skema arsitektur sistem secara menyeluruh dapat dilihat pada Gambar 1.



Gambar 1. Arsitektur Sistem

Berdasarkan Gambar 1, alur akses sistem dibedakan menjadi dua jalur utama, yaitu jalur pengguna dan jalur administrator. Pada jalur pengguna, permintaan akses dikirim melalui protokol HTTPS menuju infrastruktur Cloudflare Edge. Selanjutnya, koneksi diteruskan melalui mekanisme secure tunnel menggunakan Cloudflare Tunnel yang membangun koneksi *outbound* terenkripsi dari server internal ke jaringan Cloudflare. Lalu lintas yang telah tervalidasi kemudian diteruskan ke aplikasi Nextcloud pada server internal BBWS tanpa membuka *port* publik pada jaringan lokal.

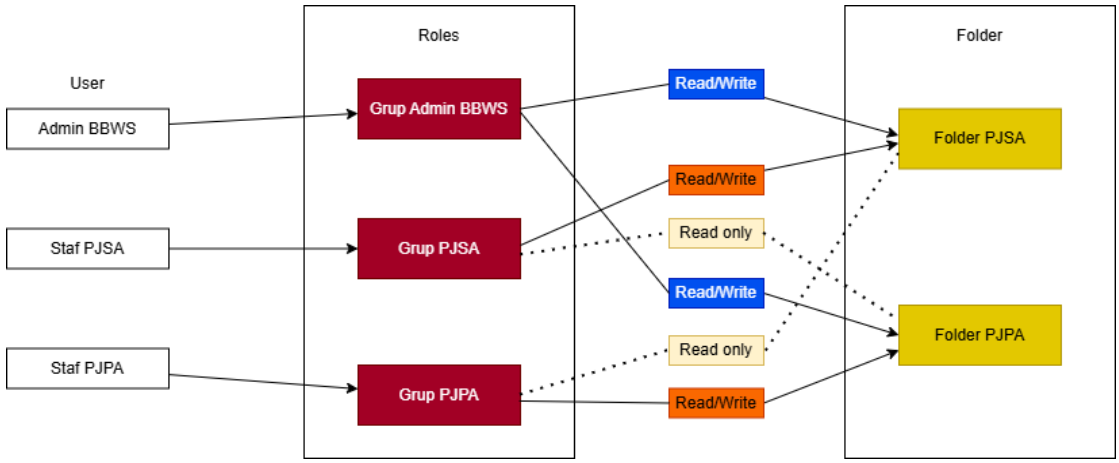
Sementara itu, akses administrator tidak dirutekan melalui domain publik. Jalur administratif dirancang terpisah menggunakan *Virtual Private Network* yaitu Tailscale. Jalur khusus ini memungkinkan administrator melakukan koneksi langsung ke antarmuka jaringan internal untuk keperluan konfigurasi TrueNAS maupun pemeliharaan server tanpa harus mengekspos jalur lalu lintas publik.

2.4 *Role-Based Access control*

Role-Based Access Control merupakan model kontrol akses yang mengatur hak akses pengguna berdasarkan peran atau fungsi tertentu dalam suatu

organisasi [3]. Model ini terdiri dari tiga komponen utama, yaitu pengguna, peran, dan izin. Pendekatan RBAC dinilai lebih fleksibel dan terstruktur dibandingkan model kontrol akses lainnya karena memudahkan pengelolaan hak akses serta meningkatkan keamanan sistem dengan membatasi akses hanya kepada pihak yang berwenang [4].

Pada sistem arsip digital BBWS Mesuji Sekampung, pengaturan hak akses dokumen diimplementasikan menggunakan model RBAC melalui fitur Team Folders pada platform Nextcloud. Model ini digunakan untuk mengelompokkan pengguna berdasarkan peran atau bidang kerja, sehingga pemberian izin akses tidak dilakukan secara individual, melainkan berbasis grup tingkat peran. Pendekatan ini secara langsung mendukung prinsip *least privilege*, di mana setiap pengguna hanya memperoleh hak akses minimum yang mutlak diperlukan untuk menjalankan tugasnya secara aman. Skema hubungan antara pengguna, peran, dan izin akses terhadap direktori folder disajikan pada Gambar 2.



Gambar 2. Arsitektur Role-Based Access Control

Berdasarkan skema tersebut, pengguna diklasifikasikan ke dalam beberapa grup sesuai struktur organisasi BBWS Mesuji Sekampung, yaitu PJSA, PJPA, O&P, SISDA, KPISDA, dan Umum & TU. Setiap grup diberikan hak akses penuh (Read/Write) terhadap direktori bidangnya masing-masing untuk mendukung pengelolaan dokumen operasional. Sementara itu, akses terhadap direktori milik bidang lain dibatasi menjadi hanya baca (*Read Only*) guna menjaga integritas data serta mencegah modifikasi yang tidak disengaja. Penetapan kewenangan akses secara spesifik untuk seluruh grup pengguna dirincikan melalui matriks hak akses pada Tabel 3.

Tabel 3. Matriks Hak Akses Pengguna

Grup	Arsip	O&P	KPISDA	SISDA	PJPA	PJSA	Umum & Tata Usaha
Admin BBWS	*R/W*	*R/W*	*R/W*	*R/W*	*R/W*	*R/W*	*R/W*
Grup Arsip	*R/W*	*RO*	*RO*	*RO*	*RO*	*RO*	*RO*
Grup O&P	*RO*	*R/W*	*RO*	*RO*	*RO*	*RO*	*RO*
Grup KPISDA	*RO*	*RO*	*R/W*	*RO*	*RO*	*RO*	*RO*
Grup SISDA	*RO*	*RO*	*RO*	*R/W*	*RO*	*RO*	*RO*
Grup PJPA	*RO*	*RO*	*RO*	*RO*	*R/W*	*RO*	*RO*
Grup PJSA	*RO*	*RO*	*RO*	*RO*	*RO*	*R/W*	*RO*
Grup Umum dan Tata Usaha	*RO*	*RO*	*RO*	*RO*	*RO*	*RO*	*R/W*

Matriks tersebut menunjukkan bahwa akun administrator memiliki hak penuh terhadap seluruh direktori, sedangkan grup pengguna lainnya hanya memiliki hak tulis pada folder bidangnya sendiri dan akses baca pada bidang lain. Struktur ini memastikan adanya segmentasi akses yang jelas serta meminimalkan risiko kesalahan operasional maupun perubahan data tanpa otorisasi.

Dengan pendekatan berbasis grup, manajemen hak akses menjadi lebih efisien karena perubahan struktur organisasi atau penambahan pengguna cukup dilakukan pada level grup tanpa perlu konfigurasi ulang pada setiap direktori secara individual. Implementasi RBAC ini juga memperkuat kontrol internal terhadap distribusi dan modifikasi arsip digital lintas bidang.

2.5 *Multi-Factor Authentication* (MFA)

Selain pengaturan hak akses berbasis peran, sistem diperkuat dengan mekanisme autentikasi berlapis melalui penerapan *Multi-Factor Authentication*. MFA dirancang secara spesifik untuk mengatasi keterbatasan autentikasi tunggal yang hanya bergantung pada hafalan kata sandi (*something you know*), yang rentan diretas akibat kebocoran kredensial [6]. Implementasi ini difokuskan pada akun administrator yang memiliki hak akses penuh terhadap seluruh direktori sistem, sehingga secara logis memerlukan tingkat perlindungan keamanan yang jauh lebih tinggi dibandingkan akun pengguna biasa.

Secara teknis, pelindungan ini diterapkan dalam bentuk *Two-Factor Authentication* dengan menambahkan verifikasi berbasis kepemilikan objek fisik (*something you have*). MFA diimplementasikan menggunakan algoritma *Time-Based One-Time Password*, yang membuat kode

autentikasi numerik dinamis dengan mengombinasikan kunci rahasia (*secret key*) dan stempel waktu saat ini (*current timestamp*) melalui fungsi *Keyed-Hash Message Authentication Code* (HMAC) [6]. Setelah proses validasi nama pengguna dan kata sandi berhasil, sistem mewajibkan administrator untuk memasukkan kode TOTP yang dihasilkan oleh aplikasi autentikator pada perangkat seluler pribadi mereka.

Penggunaan TOTP dipilih karena kemampuannya menghasilkan kode unik yang akan berubah secara otomatis dalam interval waktu yang sangat terbatas (umumnya 30 detik). Karakteristik dinamis ini secara signifikan mengurangi risiko penyalahgunaan kredensial. Dengan pendekatan ini, meskipun kata sandi utama diketahui oleh pihak penyerang, akses ke dalam sistem utama tetap tidak dapat dieksekusi tanpa adanya verifikasi kode autentikasi tambahan dari perangkat fisik milik administrator yang sah.

2.6 *Transport Layer Security*

Seluruh komunikasi data pada sistem diamankan menggunakan enkripsi *Transport Layer Security* (TLS) untuk menjaga kerahasiaan dan integritas informasi. Mekanisme ini beroperasi melalui TLS *Handshake Protocol* untuk negosiasi kunci keamanan, dilanjutkan dengan TLS *Record Protocol* yang mengenkripsi data menggunakan algoritma AES dan memverifikasi pesan melalui SHA-256 [7]. Dengan dukungan sertifikat digital Cloudflare, pertukaran data sensitif seperti kredensial dan arsip dipastikan terlindungi dari ancaman penyadapan.

2.5 *Domain Name System*

Domain Name System merupakan sistem penamaan berbasis basis data terdistribusi yang berfungsi menerjemahkan nama domain menjadi alamat IP dan sebaliknya, sehingga memudahkan pengguna dalam mengakses layanan jaringan tanpa harus mengingat alamat IP numerik [8]. DNS menerapkan struktur hierarki yang dibagi ke dalam beberapa zona untuk menjaga ketersediaan layanan, keandalan, dan memberikan konsistensi penamaan dalam sistem jaringan.

Entri data di dalam DNS disimpan dalam bentuk DNS *Resource Record*, yang berfungsi menyediakan informasi teknis yang berkaitan dengan suatu domain atau host [9]. Dalam arsitektur arsip digital ini, *record* utama yang dikonfigurasi adalah CNAME (*Canonical Name*) *Record*, yang berfungsi membuat alias dengan mengarahkan domain utama instansi (bbws-arsip.online) menuju alamat virtual tunnel milik Cloudflare.

2.5 Cloudflare Tunnel

Cloudflare Tunnel merupakan mekanisme pengamanan yang memungkinkan layanan atau aplikasi internal dapat diakses dari internet tanpa mengekspos alamat IP server secara langsung [10]. Teknologi ini bekerja dengan membangun koneksi terenkripsi antara server internal dan jaringan Cloudflare, sehingga setiap permintaan dari pengguna tidak langsung menuju server, melainkan diproses terlebih dahulu melalui infrastruktur Cloudflare. Dengan mekanisme tersebut, akses langsung ke server dapat dibatasi, sementara seluruh lalu lintas dialihkan melalui sistem Cloudflare yang telah dilengkapi berbagai fitur keamanan.

Pada implementasinya di BBWS Mesuji Sekampung, konfigurasi dilakukan dengan menginstal layanan cloudflared sebagai *connector* yang membangun terowongan (*secure tunnel*) berbasis koneksi *outbound* dari server internal menuju Cloudflare Edge. Pendekatan ini meniadakan kebutuhan konfigurasi *port forwarding* pada router atau *firewall* instansi. Seluruh permintaan akses dari pengguna eksternal akan diinspeksi terlebih dahulu oleh infrastruktur Cloudflare sebelum diteruskan ke aplikasi Nextcloud pada jaringan internal, sehingga memastikan alamat IP server tetap tersembunyi.

Selanjutnya, akses sistem dilakukan melalui domain resmi yang telah dikonfigurasi pada panel kontrol Cloudflare dengan penerapan protokol HTTPS berbasis *Transport Layer Security* (TLS). Selain enkripsi jalur komunikasi, diterapkan pula kebijakan pembatasan akses untuk memastikan bahwa hanya lalu lintas yang telah tervalidasi yang diizinkan untuk menjangkau layanan aplikasi.

2.8 Layanan Notifikasi SMTP

Simple Mail Transfer Protocol (SMTP) merupakan protokol standar yang dirancang untuk pengiriman surat elektronik (email) melalui jaringan internet [11]. Mekanisme pengiriman ini beroperasi dengan meneruskan pesan dari klien aplikasi pengirim ke server SMTP, yang kemudian mengidentifikasi alamat dan menyalurkannya melalui jaringan hingga diterima oleh klien penerima. Dalam pengembangan sistem ini, integrasi layanan SMTP dilakukan menggunakan platform pihak ketiga, yaitu Brevo, yang berfungsi sebagai SMTP *relay* untuk mendukung pengiriman email transaksional [12]. Integrasi ini diimplementasikan secara khusus untuk membangun jalur komunikasi otomatis antara sistem dan pengguna, terutama dalam pengiriman notifikasi pemulihan kata sandi secara mandiri.

Ketika pengguna mengajukan permintaan reset melalui halaman login, aplikasi Nextcloud secara otomatis mengirimkan email berisi tautan pemulihan ke alamat yang telah terdaftar. Tautan tersebut mengarahkan pengguna kembali ke halaman pengaturan ulang kata sandi yang sah pada sistem. Proses ini dipastikan hanya dapat dilakukan oleh pengguna yang memiliki akses

langsung ke email terverifikasi, sehingga mekanisme pemulihan akun tetap berada dalam kendali penuh pemilik yang sah dan terhindar dari pengambilalihan paksa.

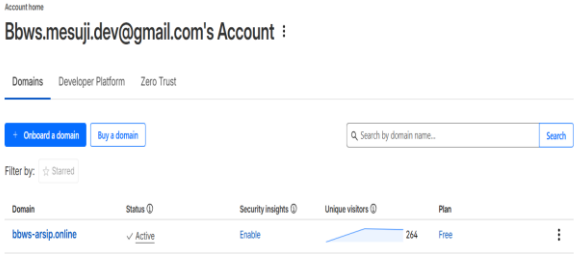
Dengan beroperasinya layanan SMTP *relay* yang terintegrasi ini, proses pemulihan kredensial dapat dieksekusi oleh pengguna tanpa memerlukan bantuan langsung dari administrator. Pendekatan ini secara signifikan meningkatkan efisiensi operasional manajemen akun sekaligus menjaga keberlangsungan akses terhadap sistem arsip digital secara aman dan terkontrol.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi sistem arsip digital beserta analisis terhadap efektivitas mekanisme manajemen akses dan keamanan yang diterapkan di lingkungan BBWS Mesuji Sekampung. Evaluasi dilakukan melalui pengujian fungsional terhadap komponen utama sistem, meliputi pengamanan koneksi berbasis HTTPS/TLS, penerapan *Role-Based Access Control*, autentikasi berlapis menggunakan *Multi-Factor Authentication*, serta mekanisme pemulihan kata sandi melalui layanan SMTP.

3.1 Implementasi Domain Cloudflare

Tahap awal pengamanan akses sistem dilakukan melalui pendaftaran dan integrasi domain bbws-arsip.online pada platform Cloudflare. Berdasarkan hasil konfigurasi, domain tersebut telah berstatus Active, yang mengindikasikan bahwa manajemen lalu lintas jaringan telah sepenuhnya dikelola oleh layanan Cloudflare.

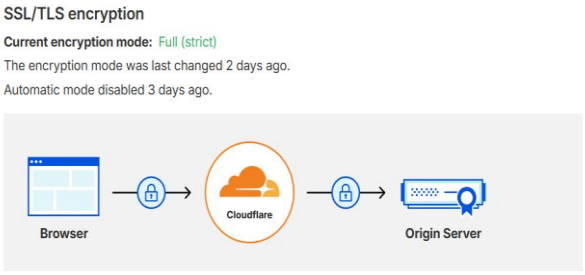


Gambar 3 Hasil integrasi domain

Integrasi ini difungsikan sebagai akses menuju website Nextcloud. Melalui mekanisme *reverse proxy*, setiap permintaan akses dari pengguna akan dirutekan dan diinspeksi oleh infrastruktur Cloudflare terlebih dahulu sebelum diteruskan ke server internal. Pendekatan ini secara efektif menyembunyikan alamat IP dari jaringan internet, sehingga mempersempit celah serangan langsung. Secara arsitektural, konfigurasi domain ini menjadi fondasi bagi penerapan mekanisme keamanan di BBWS Mesuji Sekampung, seperti pemberlakuan koneksi terenkripsi dan pengaturan kebijakan.

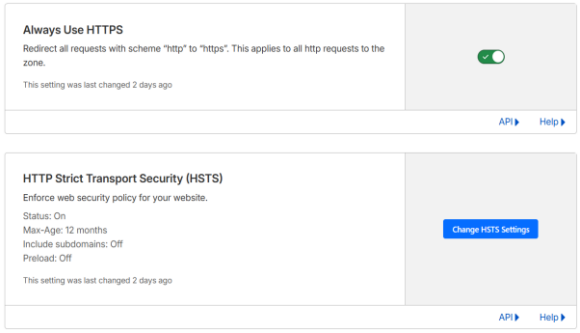
3.2 Implementasi Keamanan Koneksi dan Pembatasan Akses

Untuk melindungi komunikasi data antara pengguna dan server arsip digital, dilakukan konfigurasi keamanan koneksi menggunakan fitur SSL/TLS pada platform Cloudflare dengan mode enkripsi Full (Strict). Mode ini memastikan seluruh pertukaran data dari klien hingga ke server asal berlangsung secara terenkripsi menggunakan sertifikat yang valid, sehingga meminimalisir risiko penyadapan selama transmisi.



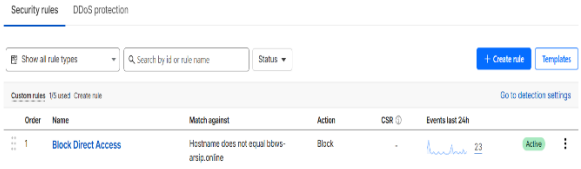
Gambar 4 Konfigurasi mode enkripsi

Selanjutnya, kebijakan *Always Use* HTTPS dan *HTTP Strict Transport Security* (HSTS) dengan periode penyimpanan 12 bulan diaktifkan. Pengaturan ini secara otomatis mengalihkan seluruh permintaan HTTP ke HTTPS dan memaksa perangkat pengguna untuk menolak koneksi yang tidak aman pada akses berikutnya.



Gambar 5 Pengaktifan HTTPS dan HSTS

Sebagai lapisan pengamanan awal sebelum permintaan diteruskan ke aplikasi Nextcloud, diterapkan pembatasan akses memanfaatkan fitur *Custom Security Rules*. Aturan keamanan ini dikonfigurasi untuk memblokir secara otomatis setiap permintaan akses yang tidak menggunakan domain resmi bbws-arsip.online.



Gambar 6 Penerapan *Custom Security Rules*

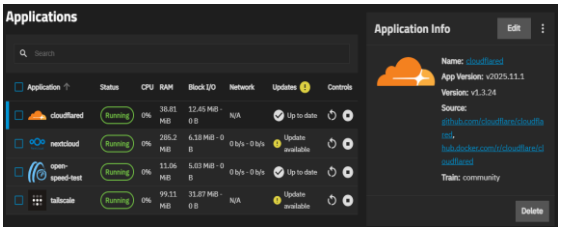
Mekanisme filter ini memastikan bahwa layanan aplikasi hanya dapat dijangkau melalui jalur domain yang telah tervalidasi. Dengan demikian, akses langsung menggunakan alamat IP publik atau

hostname lain secara tegas ditolak, yang secara signifikan melindungi infrastruktur server dari eksposur langsung ke jaringan publik dan berbagai potensi serangan siber otomatis (*automated bot attacks*).

3.3 Implementasi Cloudflare Tunnel

Untuk menghubungkan aplikasi Nextcloud dengan infrastruktur Cloudflare tanpa alamat IP publik ke internet, diimplementasikan arsitektur keamanan Cloudflare Tunnel. Konfigurasi diawali dengan membuat *tunnel token* pada *dashboard* Cloudflare yang kemudian ditambahkan ke dalam *daemon* cloudflared yang berjalan sebagai aplikasi *container* di server TrueNAS. Pendekatan koneksi *outbound* ini memungkinkan server membuat terowongan aman tanpa perlu membuka *port* layanan (*port forwarding*) pada jaringan lokal BBWS Mesuji Sekampung.

Gambar 7 Konfigurasi Cloudflare Tunnel

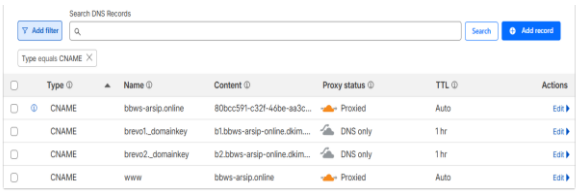


Gambar 8 Cloudflared terinstal di TrueNAS

Agar Nextcloud dapat menerima lalu lintas proksi dari terowongan ini tanpa memunculkan peringatan keamanan *untrusted domain*, domain bbws-arsip.online didaftarkan ke dalam parameter *trusted_domains* pada berkas konfigurasi aplikasi. Sebagai tahap akhir perutean, sistem Cloudflare secara otomatis menerbitkan DNS *record* bertipe CNAME yang memetakan domain utama instansi ke alamat virtual terowongan (.cfargotunnel.com). Mekanisme DNS ini merupakan inti pengamanan jaringan pada arsitektur, karena memastikan seluruh lalu lintas pengguna dirutekan secara terselubung, bukan mengarah langsung ke IP fisik server instansi.

```
'trusted_domains' =>
array (
  0 => '100.88.218.20',
  1 => '127.0.0.1',
  2 => 'bbws-arsip.online',
  3 => 'localhost',
  4 => 'nextcloud',
),
```

Gambar 9 Trusted Domains



Gambar 10 DNS *Record*s

3.4 Implementasi *Role-Based Access Control*

Untuk mengatur hak akses pengguna secara terstruktur dan membatasi eksposur data silang, diterapkan model otorisasi RBAC. Implementasi ini memanfaatkan fitur Groups dan Team Folders pada server Nextcloud untuk memetakan kewenangan secara spesifik berdasarkan struktur divisi. Pengguna diklasifikasikan ke dalam grup yang merepresentasikan bidang kerjanya di lingkungan BBWS Mesuji Sekampung, meliputi bidang Arsip, SISDA, KPISDA, O&P, PJPA, PJSA, serta Umum dan Tata Usaha.

Gambar 11 Konfigurasi RBAC

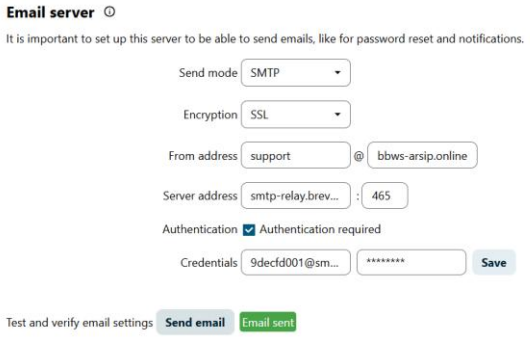
Setiap grup bidang tersebut di buat dalam sebuah Team Folder tersendiri yang berfungsi sebagai direktori penyimpanan arsip masing-masing bidang. Pengendalian hak otorisasi dikonfigurasi secara terpusat pada tingkat direktori, di mana anggota suatu grup diberikan hak akses penuh (*Read/Write*) secara eksklusif pada folder bidang mereka sendiri. Sebaliknya, akses terhadap direktori milik bidang lain dibatasi secara ketat sesuai dengan kebijakan keamanan instansi (menjadi hanya-baca atau *Read Only*). Pendekatan berbasis grup ini memastikan pengelolaan izin arsip berlangsung secara efisien dan terukur, mengeliminasi kebutuhan konfigurasi hak akses secara individual untuk setiap pengguna.

3.5 Implementasi SMTP

Untuk mendukung otomasi pengelolaan akun dan meminimalkan ketergantungan staf pada intervensi administrator, diimplementasikan layanan *Simple Mail Transfer Protocol* Konfigurasi ini diintegrasikan pada server Nextcloud guna menangani mekanisme pemulihan kredensial mandiri (*self-service password reset*).

Secara teknis, server dihubungkan dengan layanan SMTP eksternal (Brevo) melalui *port* 465 yang berjalan di atas protokol enkripsi SSL/TLS. Enkripsi transmisi ini krusial untuk mencegah

intersepsi (*sniffing*) terhadap tautan pemulihan sandi yang bersifat sangat sensitif. Selain itu, sistem dikonfigurasi untuk menggunakan alamat surel pengirim berdomain resmi instansi. Langkah ini tidak hanya memperkuat legitimasi dan kepercayaan pengguna terhadap notifikasi sistem, tetapi juga memastikan pesan tidak ditandai sebagai *spam* oleh klien surel penerima.

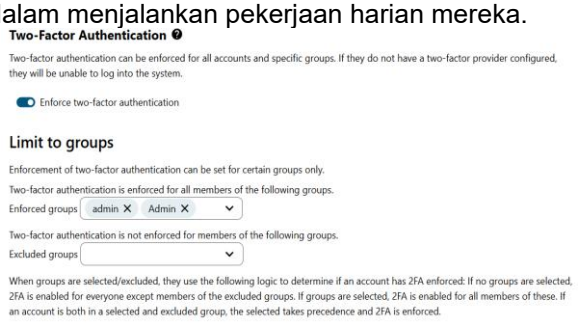


Gambar 12 Konfigurasi SMTP

3.6 Implementasi *Multi-Factor Authentication*

Untuk perlindungan, sistem ini dilengkapi fitur *Multi-Factor Authentication* melalui modul *Two-Factor Authentication* bawaan. Adanya verifikasi kedua selain kata sandi ini sangat penting untuk mencegah penyusupan.

Secara teknis, pengaturan 2FA diaktifkan dan diwajibkan khusus untuk pengguna di grup Administrator dan Admin BBWS saja. Kebijakan ini sengaja dilakukan untuk menyeimbangkan yang pas antara keamanan tingkat tinggi pada akun-akun penting dan kenyamanan akses bagi staf umum dalam menjalankan pekerjaan harian mereka.

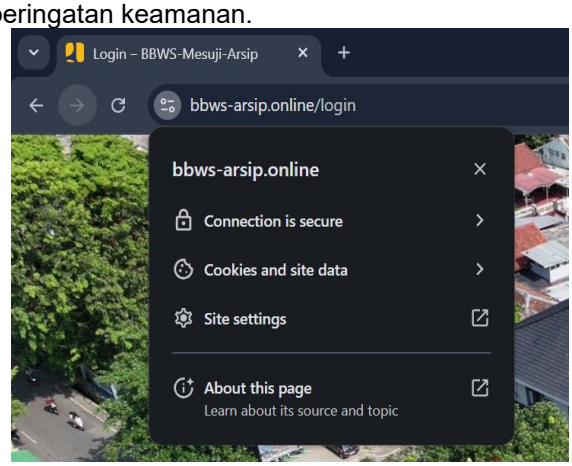


Gambar 13 *Two-Factor Authentication*

3.7 Pengujian Akses Domain

Pengujian keamanan akses domain dilakukan untuk memverifikasi bahwa layanan arsip digital hanya dapat diakses melalui koneksi terenkripsi menggunakan protokol *Hypertext Transfer Protocol Secure* (HTTPS) dengan dukungan TLS. Pengujian ini bertujuan untuk memastikan bahwa seluruh komunikasi antara klien dan server terlindungi dari potensi penyadapan serta serangan.

Pengujian dilakukan dengan mengakses halaman login sistem melalui domain resmi yang telah dikonfigurasi pada Cloudflare Tunnel. Status keamanan koneksi diperiksa menggunakan fitur inspeksi keamanan pada peramban web untuk memvalidasi penggunaan protokol HTTPS, keabsahan sertifikat digital, serta tidak adanya peringatan keamanan.



Gambar 14. Pengujian Akses Domain

Berdasarkan hasil pengujian pada Gambar 14, koneksi ke domain sistem dinyatakan aman (*connection is secure*) dan menggunakan sertifikat digital yang valid. Seluruh permintaan akses secara otomatis diarahkan ke HTTPS melalui kebijakan Always Use HTTPS dan penerapan *HTTP Strict Transport Security* (HSTS). Dengan konfigurasi ini, akses melalui protokol HTTP tidak terenkripsi tidak diizinkan.

Dari sisi arsitektur, mekanisme ini bekerja bersama Cloudflare Tunnel yang membangun koneksi *outbound* terenkripsi dari server internal ke jaringan Cloudflare. Pendekatan tersebut tidak hanya memastikan enkripsi komunikasi, tetapi juga mencegah eksposur langsung layanan aplikasi ke internet publik. Kombinasi antara TLS dan secure tunnel ini memperkuat lapisan keamanan jaringan pada sistem arsip digital.

Temuan ini menunjukkan bahwa konfigurasi SSL/TLS telah diterapkan secara konsisten dan mendukung perlindungan kerahasiaan serta integritas data pengguna selama proses transmisi.

3.8 Pengujian *Role-Based Access Control*

Pengujian RBAC dilakukan untuk memverifikasi bahwa implementasi hak akses berbasis peran telah berjalan sesuai dengan matriks desain yang disusun pada Bab 2. Evaluasi difokuskan pada validasi pembatasan akses antar direktori serta kemampuan sistem dalam mencegah modifikasi data oleh pengguna yang tidak memiliki kewenangan.

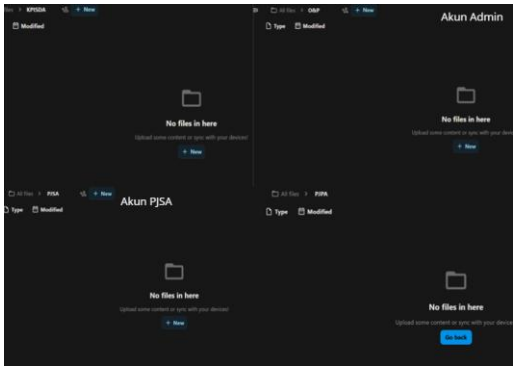
Pengujian dilakukan dengan mensimulasikan beberapa skenario akses menggunakan akun administrator dan akun perwakilan dari masing-masing grup bidang. Parameter yang diuji meliputi hak baca (*read*), hak tulis (*write*), serta percobaan modifikasi lintas direktori. Hasil pengujian dirangkum pada Tabel 4.

Tabel 4. Hasil Pengujian Implementasi RBAC

Peran	Folder Sendiri	Folder Bidang Lain	Modifikasi Lintas Bidang
Administrator	Read/Write	Read/Write	Diizinkan
Pengguna Grup	Read/Write	Read Only	Ditolak

Hasil pengujian menunjukkan bahwa sistem secara konsisten menerapkan pembatasan akses sesuai konfigurasi yang telah ditetapkan. Administrator memiliki hak penuh terhadap seluruh direktori, sedangkan pengguna hanya memiliki hak tulis pada folder bidangnya sendiri. Akses terhadap direktori bidang lain dibatasi menjadi *read-only*, dan percobaan modifikasi lintas bidang secara otomatis ditolak oleh sistem.

Perbandingan tampilan hak akses antara administrator dan pengguna ditunjukkan pada Gambar 15.



Gambar 15. Penggujian RBAC

Secara visual, Gambar 15 memperlihatkan perbedaan kewenangan antar peran sesuai skema RBAC yang diimplementasikan. Segmentasi akses ini memastikan bahwa interaksi pengguna terhadap arsip digital tetap berada dalam batas tanggung jawabnya masing-masing.

Dari perspektif keamanan, penerapan RBAC berhasil membatasi risiko kesalahan operasional maupun manipulasi data lintas bidang. Dengan pendekatan berbasis grup, pengelolaan hak akses juga menjadi lebih terstruktur dan efisien, karena perubahan kewenangan dapat dilakukan pada level peran tanpa konfigurasi ulang pada setiap direktori secara individual. Temuan ini menunjukkan bahwa mekanisme kontrol akses telah berjalan efektif dalam mendukung tata kelola arsip digital yang aman dan tersegmentasi.

3.9 Pengujian *Multi-Factor Authentication*

Pengujian MFA dilakukan untuk memverifikasi efektivitas mekanisme autentikasi berlapis dalam melindungi akun dengan hak administratif pada sistem Nextcloud. Implementasi MFA bertujuan untuk memastikan bahwa akses sistem tidak hanya bergantung pada satu faktor autentikasi berupa nama pengguna dan kata sandi, tetapi juga memerlukan verifikasi tambahan berbasis kode dinamis.

Fitur 2FA bawaan Nextcloud diaktifkan dan diterapkan secara wajib pada akun administrator. Setelah aktivasi, sistem secara otomatis meminta konfigurasi metode autentikasi tambahan menggunakan algoritma TOTP melalui aplikasi autentikator. Proses login tidak dapat dilanjutkan sebelum konfigurasi MFA diselesaikan, yang menunjukkan bahwa kebijakan autentikasi berlapis diterapkan secara konsisten pada akun dengan hak istimewa tinggi.

Pengujian dilakukan dengan melakukan proses login menggunakan kombinasi kredensial yang benar dan kode TOTP yang valid. Hasil pengujian menunjukkan bahwa akses hanya diberikan ketika kode TOTP sesuai dengan kode yang dihasilkan aplikasi autentikator pada interval waktu yang berlaku.

Gambar 16. Proses verifikasi kode autentikasi TOTP

Berdasarkan Gambar 16, sistem secara eksplisit meminta verifikasi kode autentikasi tambahan sebelum memberikan akses ke *dashboard* administrator. Mekanisme ini menambahkan lapisan proteksi terhadap risiko penyalahgunaan kredensial, karena kepemilikan kata sandi saja tidak cukup untuk memperoleh akses sistem.

Dari perspektif keamanan, penerapan MFA berbasis TOTP meningkatkan ketahanan sistem terhadap serangan berbasis pencurian kata sandi (*credential compromise*) dan *brute force attack*. Dengan kombinasi autentikasi dua faktor, potensi akses tidak sah terhadap direktori arsip digital dapat diminimalkan secara signifikan.

3.10 Pengujian Reset Kata Sandi

Pengujian reset kata sandi dilakukan untuk memverifikasi keberhasilan integrasi antara aplikasi Nextcloud dan layanan *Simple Mail Transfer Protocol* yang telah dikonfigurasikan. Evaluasi ini bertujuan untuk memastikan bahwa mekanisme pemulihan akun dapat berjalan secara mandiri, terkontrol, dan tetap memenuhi aspek keamanan.

Pengujian diawali dengan mengajukan permintaan reset melalui halaman login menggunakan akun yang telah terdaftar pada sistem. Setelah permintaan dikirimkan, sistem secara otomatis mengirimkan email berisi tautan

pemulihan ke alamat pengguna yang bersangkutan. Tautan tersebut mengarahkan pengguna ke halaman pengaturan ulang kata sandi sebagaimana ditunjukkan pada Gambar 17.

Gambar 17. Reset Kata Sandi

Tautan pemulihan hanya dapat diakses oleh pengguna yang memiliki kontrol terhadap alamat email terdaftar dan berlaku dalam periode waktu tertentu sesuai konfigurasi sistem. Mekanisme ini membatasi potensi penyalahgunaan permintaan reset oleh pihak yang tidak berwenang.

Hasil pengujian menunjukkan bahwa proses pengiriman email berjalan dengan baik, tautan pemulihan dapat diakses secara valid, dan pembaruan kata sandi berhasil dilakukan tanpa kendala. Setelah kata sandi diperbarui, pengguna dapat kembali mengakses sistem menggunakan kredensial baru.

Dari perspektif keamanan, mekanisme ini meningkatkan kemandirian pengguna dalam pengelolaan akun sekaligus mempertahankan kontrol akses berbasis verifikasi email. Integrasi SMTP yang stabil juga mendukung kontinuitas operasional sistem arsip digital dengan meminimalkan ketergantungan terhadap intervensi administrator.

4. KESIMPULAN

Adapun kesimpulan dari laporan ini adalah sebagai berikut:

1. Penerapan *Role-Based Access Control* mengatur akses pengguna berdasarkan peran dan bidang kerja. Mekanisme ini membatasi pengguna hanya mengelola dokumen yang relevan, sehingga keamanan data dan keteraturan arsip antarbidang lebih terjamin.
2. Implementasi Cloudflare Tunnel mengamankan akses publik tanpa perlu membuka *port* server secara langsung. Dengan dukungan enkripsi TLS, jalur komunikasi terlindungi sehingga meminimalkan risiko penyadapan maupun serangan dari jaringan luar.
3. Penerapan *Multi-Factor Authentication* dalam bentuk *Two-Factor Authentication* pada akun administratif sebagai bagian dari penguatan keamanan sistem memberikan perlindungan tambahan pada proses login. Verifikasi tambahan ini membantu mengurangi risiko penyalahgunaan akun dengan hak istimewa akibat kebocoran kata sandi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Balai Besar Wilayah Sungai (BBWS) Mesuji Sekampung atas dukungan dan fasilitas yang diberikan selama pelaksanaan kerja praktik. Ucapan terima kasih juga disampaikan kepada Bapak Faris Haidi, S.T., selaku pembimbing lapangan, atas arahan dan dukungan teknis selama proses implementasi sistem. Selain itu, penulis menyampaikan terima kasih kepada Bapak Ir. Gigih Forda Nama, S.T., M.T.I., selaku dosen pembimbing, serta Bapak Rio Ariestia Pradipta, S.Kom., M.T.I., selaku dosen penguji, atas arahan dan masukan dalam penyempurnaan artikel ini.

DAFTAR PUSTAKA

[1] M. I. Herdiansyah and H. Novendra, “Analisis Pemanfaatan TrueNAS Pada BKN Kanreg VII Palembang,” *Jurnal Pengembangan Sistem Informasi dan Informatika*, vol. 5, no. 2, 2024.

[2] A. Irawan, A. Purnama Sari, and S. Bahri, “PERANCANGAN DAN IMPLEMENTASI CLOUD STORAGE MENGGUNAKAN NEXTCLOUD PADA SMK YPP PANDEGLANG,” *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, vol. 5, no. 2, 2019.

[3] Rubiyanto, Selo, and Widyawan, “IMPLEMENTASI ROLE-BASED ACCESS CONTROL (RBAC) PADA PEMANFAATAN DATA KEPENDUDUKAN DITINGKAT KABUPATEN,” in *Seminar Nasional Sains dan Teknologi (SEMNASTEK)*, Jakarta: Fakultas Teknik UMJ, 2017, pp. 1–10.

[4] M Sahyudi and E. R. Susanto, “Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning,” *SATESI: Jurnal Sains Teknologi dan Sistem Informasi*, vol. 5, no. 1, pp. 105–116, 2025, doi: 10.54259/satesi.v5i1.3997.

[5] Z. A. Bahalwan and D. Febriawan, “Implementasi Server Cloud Storage Menggunakan SFTPGo, Docker, dan Cloudflare Tunnel,” *Jurnal Teknik Informatika dan Komputer*, vol. 4, no. 2, pp. 71–76, 2025.

[6] A. Y. Fitriyansyah and M. Hazri, “Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One-Time Password,” *Jurnal Mahasiswa Teknik Informatika*, vol. 7, no. 4, pp. 2938–2945, 2023.

[7] W. S. Raharjo and A. A. Bajuadji, “Analisa Implementasi Protokol HTTPS pada Situs Web Perguruan Tinggi di Pulau Jawa,” *Ultimatics : Jurnal Teknik Informatika*, vol. 8, no. 2, 2016.

[8] A. Tedyyana and R. Kurniati, “MEMBUAT WEB SERVER MENGGUNAKAN DINAMIC DOMAIN NAME SYSTEM PADA IP DINAMIS,” *Jurnal Teknologi Informasi & Komunikasi Digital Zone*, vol. 7, no. 1, pp. 1–10, 2016.

[9] A. Tanenbaum and D. Wetherall, *Computer Networks 5th Edition*, 5th ed. Pearson, 2011.

[10] P. Jaisudthi, P. Threerapat Sridee, N. Phungkoed, K. Srisuk, and V. Phueaknumpol, “Comparative Study of Modern VPN Solutions: Impact of Cloudflare, ZeroTier, and WireGuard on Network and Server Performance,” *Engineering and Technology Horizons*, vol. 42, no. 2, 2025, doi: 10.55003/ETH.420203.

[11] M. A. Adiguna, “Pemanfaatan SMTP Client pada Sistem Absensi VB.Net,” *Jurnal Teknologi dan Informasi*, vol. 10, no. 2, pp. 108–115, 2020, doi: 10.34010/jati.v10i2.

[12] Brevo, “Send transactional emails using Brevo SMTP,” Brevo Help Center. Accessed: Dec. 27, 2025. [Online]. Available: https://help.brevo.com/hc/en-us/articles/7924908994450-Send-transactional-emails-using-Brevo-SMTP