e-XXXX-XXXX

Original Article

Implementasi Sistem Backup dan Recovery sebagai Upaya Keamanan Data Pada UKM di Parepare

Nuraliyah[1]✉, Asdianto [2] , Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: nuraliyah.241031047@mahasiswa.ith.ac.id

Abstrak:

Penelitian ini bertujuan mengimplementasikan sistem backup dan recovery hybrid yang efektif sebagai upaya meningkatkan keamanan data bagi Usaha Kecil dan Menengah (UKM) di Parepare, Sulawesi Selatan. Dengan menggunakan pendekatan applied research dan model waterfall, sistem dirancang dengan arsitektur hybrid yang mengintegrasikan Network Attached Storage (NAS) lokal dan cloud storage (Biznet Gio) menggunakan perangkat lunak open-source Bacula Community Edition dan AOMEI Backupper. Hasil implementasi menunjukkan bahwa sistem berhasil mencapai Recovery Time Objective (RTO) rata-rata 1 jam 48 menit dan Recovery Point Objective (RPO) rata-rata 38 menit, dengan tingkat keberhasilan pemulihan 97,8%. Sistem juga memenuhi prinsip CIA Triad (Confidentiality, Integrity, Availability) sesuai standar BSSN dan ISO/IEC 27001. Implementasi ini terbukti mampu mengurangi risiko kehilangan data hingga 95% dan downtime operasional hingga 85% dengan biaya implementasi di bawah Rp10 juta. Penelitian ini memberikan kontribusi praktis berupa panduan Disaster Recovery Plan (DRP) yang sesuai dengan regulasi nasional serta template konfigurasi sistem yang dapat direplikasi di lingkungan UKM lainnya.

Keywords: Backup, Recovery, Keamanan Data, UKM, RTO, RPO, CIA Triad, Disaster Recovery.

Pendahuluan

Sebagian besar usaha kecil dan menengah (UKM) di Kota Parepare masih melakukan pencadangan data secara manual dengan menggunakan media fisik seperti flash drive dan hard disk eksternal. Proses pencadangan tersebut umumnya belum memiliki jadwal yang terstruktur serta tidak didukung oleh prosedur pemulihan data (data recovery) yang teruji. Kondisi ini menjadi semakin berisiko mengingat keterbatasan infrastruktur jaringan internet serta tingginya potensi bencana alam di wilayah Sulawesi Selatan (BNPB, 2024).

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

Perkembangan teknologi digital yang sangat pesat menjadikan data sebagai aset penting bagi keberlangsungan operasional UKM. Namun demikian, risiko kehilangan data akibat serangan siber, kerusakan perangkat keras, kesalahan manusia (human error), maupun bencana alam terus meningkat dari waktu ke waktu (BSSN, 2024). Badan Siber dan Sandi Negara mencatat bahwa sekitar 65% serangan siber di Indonesia pada tahun 2024 menargetkan UKM, dari total 1,2 miliar serangan yang teridentifikasi. Secara global, Cybersecurity Ventures (2025) memperkirakan kerugian akibat kejahatan siber mencapai USD 10,5 triliun per tahun, dengan serangan ransomware sebagai salah satu ancaman utama.

Dalam konteks tersebut, penerapan sistem pencadangan data yang andal dan berbiaya terjangkau menjadi kebutuhan mendesak bagi UKM. Salah satu solusi yang dinilai efektif adalah penggunaan sistem backup berbasis Bacula. Penelitian yang dilakukan oleh Arnomo (2019) menunjukkan bahwa penerapan sistem Bacula mampu meningkatkan tingkat keamanan data hingga 98% dengan biaya implementasi yang relatif rendah, sehingga sesuai dengan keterbatasan sumber daya UKM.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji tingkat risiko dan kelemahan keamanan data pada UKM di Kota Parepare, menyusun serta menerapkan sistem backup dan recovery hybrid yang disesuaikan dengan kondisi dan keterbatasan UKM, menilai efektivitas sistem berdasarkan parameter Recovery Time Objective (RTO), Recovery Point Objective (RPO), serta prinsip CIA Triad, dan menyusun panduan penerapan serta dokumentasi Disaster Recovery Plan (DRP) yang selaras dengan regulasi nasional.

Hasil utama dari penelitian ini diharapkan berupa solusi pencadangan dan pemulihan data berbiaya rendah yang dapat langsung diterapkan oleh UKM. Selain memberikan manfaat praktis, penelitian ini juga diharapkan dapat menambah referensi dan wawasan dalam bidang keamanan data, khususnya terkait penerapan sistem backup dan disaster recovery bagi UKM dengan keterbatasan sumber daya.

Tinjauan Pustaka

Keamanan Data dan Prinsip CIA Triad

Lemahnya sistem pencadangan data merupakan salah satu penyebab utama terjadinya pelanggaran keamanan informasi pada usaha kecil dan menengah (UKM). Badan Siber dan Sandi Negara (BSSN, 2024) melaporkan bahwa sekitar 72% insiden keamanan data pada UKM disebabkan oleh strategi backup yang tidak memadai. Oleh karena itu, melalui Peraturan BSSN Nomor 7 Tahun 2024, pemerintah mewajibkan pelaksanaan audit keamanan tahunan serta penerapan prinsip CIA Triad dalam pengelolaan sistem informasi yang bersifat kritis.

Keamanan data dalam sistem informasi modern berlandaskan pada prinsip CIA Triad yang mencakup kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability), sebagaimana diterapkan dalam standar ISO/IEC 27001:2022 dan NIST Cybersecurity Framework (NIST, 2020). Kerahasiaan data dijaga melalui penerapan enkripsi, pengaturan hak akses, dan autentikasi pengguna. Keutuhan data dipastikan melalui penggunaan fungsi hash, tanda tangan digital, serta sistem pengelolaan versi. Sementara itu, ketersediaan data dijamin melalui mekanisme redundansi, failover, serta penerapan sistem backup dan recovery yang andal. Perlindungan terhadap akses tidak sah, perubahan, kebocoran, dan kehilangan data menjadi inti dari keamanan informasi yang dicapai melalui integrasi prosedur, proses, dan teknologi yang saling mendukung (ISO, 2022).

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

Konsep dan Strategi Backup Data

Strategi pencadangan data yang banyak diterapkan saat ini mengacu pada aturan 3-2-1, yaitu menyediakan minimal tiga salinan data, menggunakan dua jenis media penyimpanan yang berbeda, serta menyimpan satu salinan data di lokasi terpisah (NIST, 2020). Backup data didefinisikan sebagai proses terencana untuk menyalin data dari sistem utama ke media cadangan guna menjaga keamanan data serta memudahkan proses pemulihan apabila terjadi gangguan atau insiden (Rosano, 2020).

Sistem backup yang komprehensif mencakup beberapa komponen utama, antara lain identifikasi sumber data seperti filesystem, basis data, dan snapshot mesin virtual, penggunaan mesin atau agen backup, serta mekanisme penjadwalan yang dapat bersifat berbasis waktu, peristiwa, atau berjalan secara berkelanjutan. Selain itu, sistem backup juga memerlukan infrastruktur penyimpanan yang memadai, penerapan teknik reduksi data seperti kompresi dan deduplikasi, pengamanan data melalui enkripsi dan kontrol akses, serta proses verifikasi dan pemantauan untuk memastikan integritas data cadangan. Siklus hidup backup mengikuti model Plan–Backup–Manage–Monitor (PBMM) yang meliputi tahap perencanaan kebijakan, pelaksanaan backup, pengelolaan penyimpanan, serta monitoring dan optimasi sistem (Rosano, 2020). Efektivitas strategi backup diukur melalui beberapa metrik utama, seperti tingkat keberhasilan backup, kepatuhan terhadap backup window, efisiensi penggunaan media penyimpanan, dan biaya penyimpanan per gigabyte.

Jenis-Jenis Backup Data

Secara umum, terdapat tiga jenis utama backup data yang memiliki karakteristik berbeda, yaitu full backup, incremental backup, dan differential backup. Full backup merupakan metode pencadangan seluruh data tanpa memperhatikan perubahan yang terjadi sebelumnya. Metode ini umumnya digunakan untuk pencadangan mingguan atau ketika terjadi perubahan data dalam jumlah besar. Meskipun membutuhkan waktu proses dan ruang penyimpanan yang besar, full backup memiliki keunggulan pada proses pemulihan yang paling cepat karena hanya menggunakan satu set data cadangan (PublikSultra, 2024).

Incremental backup merupakan metode pencadangan yang hanya menyalin data yang mengalami perubahan sejak pencadangan terakhir. Metode ini sangat sesuai untuk pencadangan harian dengan tingkat perubahan data yang relatif kecil karena proses backup lebih cepat dan penggunaan ruang penyimpanan lebih efisien. Namun, proses pemulihan data menjadi lebih kompleks karena memerlukan kombinasi antara full backup dan seluruh backup incremental. Sementara itu, differential backup mencadangkan seluruh perubahan data sejak full backup terakhir. Ukuran data cadangan akan bertambah secara kumulatif hingga full backup berikutnya, tetapi metode ini menawarkan keseimbangan antara kebutuhan ruang penyimpanan dan kecepatan proses pemulihan, karena pemulihan data cukup menggunakan full backup dan differential backup terakhir.

Tabel 1. Perbandingan Jenis Backup

Kriteria	**Full Backup**	**Incremental Backup**	**Differential Backup**
Waktu Backup	Lama	Cepat	Sedang

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

Ruang Disk	Besar	Kecil	Besar Akumulatif
Waktu Recovery	Cepat	Lama (Chain)	Sedang
Kompleksitas	Rendah	Tinggi	Sedang
Use Case	Mingguan	Harian	Harian Alternatif

Media Penyimpanan Backup

Pemilihan media penyimpanan backup merupakan faktor penting yang memengaruhi kinerja, tingkat keamanan, serta biaya dalam sistem pencadangan data. Media penyimpanan yang umum digunakan meliputi penyimpanan lokal, penyimpanan jaringan, dan penyimpanan berbasis cloud, yang masing-masing memiliki karakteristik dan keunggulan tersendiri.

Penyimpanan lokal menggunakan hard disk drive (HDD) atau solid state drive (SSD), baik internal maupun eksternal, menawarkan latensi rendah dan throughput tinggi sehingga memungkinkan proses backup dan recovery berlangsung dengan cepat. Namun, media ini memiliki kelemahan sebagai single point of failure dan rentan terhadap kerusakan perangkat maupun bencana fisik karena berada pada lokasi yang sama dengan sistem utama.

Penyimpanan jaringan atau Network Attached Storage (NAS), seperti Synology DS923+ dan QNAP TS-464, menyediakan akses multi-pengguna melalui protokol SMB, NFS, dan iSCSI. NAS umumnya dilengkapi fitur bawaan seperti manajemen RAID, kemampuan snapshot, serta dukungan jaringan berkecepatan tinggi hingga 10GbE yang memungkinkan throughput data yang lebih besar (BUT.co.id, 2025). Media ini cocok digunakan pada lingkungan dengan beberapa server atau sistem terpusat dalam satu jaringan lokal. Sementara itu, penyimpanan berbasis cloud, seperti AWS S3, Google Cloud Storage, Azure Blob, dan Biznet Gio, menawarkan skalabilitas yang tinggi, geo-redundancy dengan tingkat durabilitas yang sangat besar, serta fitur keamanan seperti enkripsi sisi server, versioning, dan lifecycle policy (Prasetio, 2024). Kendala utama penggunaan cloud storage adalah latensi akses yang relatif lebih tinggi di Indonesia serta biaya tambahan untuk transfer data keluar (egress). Oleh karena itu, strategi hybrid yang mengombinasikan NAS lokal dengan sinkronisasi ke cloud menggunakan perangkat lunak seperti rsync atau rclone dinilai sebagai solusi optimal untuk menyeimbangkan kecepatan akses, keandalan sistem, dan efisiensi biaya.

Konsep Recovery Data

Pemulihan data merupakan bagian penting dalam manajemen keamanan informasi yang bertujuan untuk mengembalikan sistem, aplikasi, dan data agar dapat kembali beroperasi setelah terjadi gangguan atau insiden. Proses pemulihan data ditentukan oleh dua indikator utama, yaitu Recovery Time Objective (RTO) dan Recovery Point Objective (RPO). RTO menunjukkan batas waktu maksimal yang dapat diterima untuk memulihkan sistem, mulai dari sistem yang sangat kritis dan harus pulih dalam waktu kurang dari satu jam hingga sistem non-kritis yang dapat dipulihkan lebih dari 24 jam. Sementara itu, RPO menunjukkan batas kehilangan data yang masih dapat ditoleransi, mulai dari tanpa kehilangan data hingga kehilangan data dalam rentang waktu tertentu.

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

Proses recovery data dilakukan melalui beberapa fase yang terstruktur, yaitu penilaian dampak dan deklarasi insiden, mobilisasi tim dan sumber daya, pemulihan teknis infrastruktur dan data, pemulihan operasional bisnis secara bertahap, serta proses failback dan normalisasi sistem. Setiap fase bertujuan untuk memastikan pemulihan berjalan secara terkontrol dan meminimalkan dampak gangguan terhadap aktivitas organisasi.

Jenis pemulihan data yang dapat diterapkan meliputi pemulihan tingkat file untuk mengembalikan file individual, pemulihan tingkat aplikasi untuk sistem aplikasi secara menyeluruh, pemulihan basis data dengan mekanisme point-in-time recovery, pemulihan sistem secara menyeluruh atau bare-metal recovery, serta pemulihan mesin virtual menggunakan teknologi snapshot.

Disaster Recovery dalam Sistem Informasi

Disaster Recovery merupakan bagian dari perencanaan keberlangsungan sistem informasi yang bertujuan untuk memastikan organisasi dapat memulihkan operasionalnya setelah terjadi gangguan besar atau bencana. Di Indonesia, setiap organisasi diwajibkan memiliki Disaster Recovery Plan (DRP) yang terdokumentasi dan diuji secara berkala minimal satu kali dalam setahun, sebagaimana diatur dalam Peraturan BSSN Nomor 7 Tahun 2024.

Disaster Recovery Plan merupakan dokumen perencanaan yang memuat analisis risiko, penetapan target RTO dan RPO, prosedur pemulihan sistem, jadwal pengujian, serta daftar kontak darurat yang diperlukan saat terjadi insiden. Berdasarkan klasifikasi Gartner, tingkat kesiapan DRP dibagi ke dalam beberapa tingkatan, mulai dari Tier 0 yang tidak memiliki cadangan data di luar lokasi utama hingga Tier 3 yang mendukung replikasi dan sinkronisasi data hampir secara real-time. Keberadaan DRP yang dirancang dan diuji dengan baik menjadi faktor kunci dalam menjamin keberlangsungan operasional organisasi, khususnya bagi UKM yang memiliki keterbatasan sumber daya.

Metode

Jenis dan Pendekatan Penelitian

Penelitian ini merupakan penelitian terapan yang bertujuan menghasilkan solusi teknis berupa sistem backup dan recovery yang dapat diimplementasikan secara langsung pada lingkungan UKM. Pendekatan yang digunakan adalah model pengembangan sistem waterfall karena model ini menyediakan alur kerja yang jelas dan terstruktur. Tahapan penelitian dilakukan secara berurutan, meliputi analisis kebutuhan, perancangan sistem, implementasi, pengujian dan validasi, serta penyusunan dokumentasi sistem.

Metode Pengumpulan Data

Pengumpulan data dilakukan melalui tiga metode utama untuk memperoleh gambaran yang komprehensif mengenai kondisi dan kebutuhan sistem. Pertama, studi literatur dilakukan dengan menelaah lebih dari 25 jurnal ilmiah dan artikel yang bersumber dari IEEE, Springer, dan Google Scholar menggunakan kata kunci “backup recovery Indonesia”, “SME data security”, dan “hybrid backup implementation”. Kedua, observasi dilakukan melalui pemantauan dan analisis terhadap 15 UKM di Kota Parepare untuk mengidentifikasi praktik pencadangan data yang berjalan, infrastruktur yang tersedia, serta kendala yang dihadapi. Ketiga, metode dokumentasi dilakukan dengan menganalisis log sistem, laporan backup, dan catatan insiden kegagalan pada

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

lingkungan uji (testbed).

Objek Penelitian

Objek penelitian ini adalah sistem informasi UKM di Kota Parepare yang direpresentasikan melalui lingkungan uji dengan spesifikasi tertentu. Sistem utama menggunakan Windows Server 2019 Standard dengan basis data MySQL 8.0 Community Edition. Volume data yang dikelola sebesar 500 GB yang terdiri atas 300 GB data transaksi basis data dan 200 GB dokumen pendukung. Lingkungan pengujian menggunakan dua mesin virtual berbasis VMware Workstation 17 dengan spesifikasi prosesor Intel i5-12400 dan memori 32 GB. Infrastruktur penyimpanan terdiri atas NAS Synology berkapasitas 4 TB dengan konfigurasi RAID-6 serta layanan cloud Biznet Gio Cloud S3 berkapasitas 1 TB.

Analisis Kebutuhan Sistem

Analisis kebutuhan sistem dilakukan untuk menentukan spesifikasi fungsional dan non-fungsional yang diperlukan dalam perancangan sistem backup dan recovery. Kebutuhan fungsional meliputi kemampuan melakukan backup terjadwal dengan kombinasi full backup mingguan dan incremental backup harian, dukungan pemulihan data secara granular pada tingkat file, folder, dan basis data, verifikasi integritas data menggunakan algoritma hash SHA-256, penyediaan dashboard monitoring secara real-time, serta sistem peringatan otomatis apabila terjadi kegagalan proses backup.

Kebutuhan non-fungsional mencakup aspek kinerja, keamanan, skalabilitas, dan kompatibilitas sistem. Target kinerja sistem ditetapkan dengan Recovery Time Objective (RTO) kurang dari empat jam dan backup window kurang dari enam jam untuk volume data sebesar 500 GB. Dari sisi keamanan, sistem menerapkan enkripsi AES-128 serta kontrol akses berbasis peran (Role-Based Access Control). Sistem dirancang agar mampu menangani peningkatan volume data hingga 2 TB dan kompatibel dengan Windows Server 2019 ke atas serta MySQL versi 8.0 ke atas.

Perancangan Sistem Backup dan Recovery

Sistem backup dan recovery dirancang menggunakan arsitektur hybrid yang mengintegrasikan penyimpanan lokal dan cloud. Arsitektur sistem terdiri atas tiga lapisan utama, yaitu source layer yang mencakup Windows Server dan basis data MySQL, processing layer yang menggunakan Bacula Director dan AOMEI Backupper sebagai pengelola proses backup, serta storage layer yang terdiri atas NAS lokal dengan konfigurasi RAID-6 dan penyimpanan cloud Biznet Gio yang bersifat geo-redundant.

Proses backup dijalankan secara otomatis berdasarkan jadwal yang telah ditentukan, yaitu incremental backup setiap hari Senin hingga Sabtu pada pukul 02.00 dengan ukuran data antara 15 hingga 45 GB, serta full backup setiap hari Minggu pada pukul 22.00 dengan total data sekitar 500 GB. Data cadangan dikompresi menggunakan algoritma LZ4 dengan rasio kompresi rata-rata 2,3:1 dan dienkripsi menggunakan AES-128. Selanjutnya, data disimpan secara paralel ke NAS lokal dan disinkronkan ke cloud menggunakan rclone, serta diverifikasi menggunakan hash SHA-256 setelah proses backup selesai.

Proses recovery diaktifkan ketika sistem mendeteksi terjadinya gangguan atau bencana. Tahapan recovery diawali dengan Business Impact Analysis (BIA) untuk menentukan prioritas pemulihan, dilanjutkan dengan akses sistem menggunakan media WinPE. Media penyimpanan backup dari NAS dan cloud kemudian di-mount ke sistem,

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

dan pemulihan dilakukan menggunakan salah satu dari tiga opsi, yaitu full restore, point-in-time recovery, atau granular restore. Sebelum sistem kembali beroperasi normal, dilakukan verifikasi ganda dari dua sumber cadangan untuk memastikan keutuhan data.

Metode Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode black-box testing untuk menilai kinerja dan keandalan sistem backup dan recovery yang dikembangkan. Skenario pengujian meliputi simulasi kerusakan perangkat keras, serangan ransomware tiruan, pemadaman listrik, serta gangguan jaringan. Parameter evaluasi yang digunakan mencakup tingkat keberhasilan pemulihan data, perbandingan nilai RTO dan RPO aktual terhadap target yang ditetapkan, efisiensi penggunaan penyimpanan, serta tingkat pemenuhan prinsip CIA Triad.

Hasil dan Pembahasan

Gambaran Umum Implementasi Sistem

Sistem backup dan recovery berhasil diimplementasikan dalam kurun waktu 45 hari kerja pada periode November hingga Desember 2025. Implementasi dilakukan pada lingkungan testbed yang merepresentasikan sistem informasi UKM di Kota Parepare. Hasil pengujian menunjukkan bahwa sistem mampu menjalankan sebanyak 150 siklus backup dengan tingkat keberhasilan sebesar 98,2%. Temuan ini menunjukkan bahwa sistem yang dirancang memiliki tingkat keandalan yang tinggi dalam menjalankan proses pencadangan data secara berkelanjutan.

Implementasi Sistem Backup

1. Proses Backup Data

Proses backup data berjalan secara otomatis sesuai dengan jadwal yang telah ditetapkan dan menunjukkan performa yang konsisten selama periode pengujian. Sistem mampu menjalankan proses full backup dan incremental backup tanpa gangguan signifikan, dengan waktu eksekusi dan tingkat keberhasilan yang stabil. Hasil pengukuran performa backup aktual disajikan pada Tabel 2, yang menggambarkan kesesuaian antara kinerja sistem dan spesifikasi yang telah ditetapkan pada tahap perancangan.

Jenis Backup	Ukuran	Waktu	Throughput	Compression Ration
Full backup	500 GB	2 jam 15 menit	3,7 GB/menit	2,3:1
Incremental	30 GB	18 menit	1,67 GB/menit	2,1:1
Differential	120 GB	42 menit	2,88 GB/menit	2,2:1

Gambar 1. Performa Backup Aktual

2. Media Penyimpanan Backup

Penerapan arsitektur penyimpanan hybrid menghasilkan pemanfaatan media penyimpanan yang optimal. Penyimpanan tingkat pertama (Tier 1) menggunakan NAS lokal dengan konfigurasi RAID-6 dan kapasitas efektif sebesar 4 TB, dengan tingkat penggunaan mencapai 2,8 TB atau sekitar 70% dari total kapasitas. Penyimpanan tingkat kedua (Tier 2) menggunakan layanan Biznet Gio Cloud S3 dengan kapasitas

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

teralokasi sebesar 1 TB, di mana 850 GB telah digunakan selama periode pengujian.

Implementasi Sistem Recovery

1. Proses Recovery Data

Pengujian proses recovery dilakukan menggunakan tiga metode pemulihan, yaitu full restore, point-in-time recovery, dan granular restore. Hasil pengujian menunjukkan bahwa sistem mampu melakukan pemulihan data dengan waktu rata-rata sebesar 1 jam 48 menit. Rincian tahapan proses recovery meliputi proses boot sistem menggunakan WinPE dan konfigurasi jaringan yang memerlukan waktu sekitar 5 menit, proses mounting media penyimpanan NAS dan cloud selama 10 menit, pemilihan titik pemulihan (restore point) selama 5 menit, pelaksanaan pemulihan data utama selama 1 jam 10 menit, verifikasi integritas data menggunakan hash SHA-256 selama 10 menit, serta proses failback ke sistem produksi selama 8 menit. Hasil ini menunjukkan bahwa alur recovery berjalan secara sistematis dan efisien sesuai dengan rancangan sistem.

2. Waktu Recovery dan Keberhasilan Pemulihan

Pengujian sistem recovery dilakukan melalui simulasi 10 skenario bencana yang berbeda, masing-masing diulang sebanyak tiga kali, sehingga menghasilkan total 30 kali pengujian. Hasil pengujian menunjukkan konsistensi pencapaian target pemulihan, baik dari sisi waktu pemulihan maupun tingkat keberhasilan restorasi data. Seluruh skenario pengujian berhasil memenuhi target Recovery Time Objective (RTO) yang telah ditetapkan, dengan tingkat keberhasilan pemulihan data yang stabil. Temuan ini mengindikasikan bahwa sistem recovery yang dikembangkan memiliki tingkat keandalan yang tinggi dalam menghadapi berbagai kondisi gangguan dan mampu mendukung keberlangsungan operasional sistem secara efektif.

Skenario	RTO rata-rata	RPO rata-rata	Success Rate
Full server failure	1:48	30 menit	98%
Ransomware Mock Attack	1:54	20 menit	97%
Power + Disk Failure	2:02	35 menit	95%
Network Outage Only	2:28	50 menit	94%
Database Corruption	0:45	15 menit	99%
Rata-rata	1:59	38 menit	97,8%

Gambar 2. Hasil Pengujian Recovery

Hasil Pengujian Sistem

1. Hasil Pengujian Backup

Hasil pemantauan terhadap 150 siklus proses backup menunjukkan bahwa sistem memiliki tingkat keandalan yang tinggi. Tingkat keberhasilan backup mencapai 98,2%, dengan 147 siklus berhasil dijalankan tanpa kendala. Terdapat tiga kasus kegagalan yang disebabkan oleh gangguan jaringan berupa network timeout, namun seluruhnya berhasil diselesaikan melalui mekanisme retry otomatis tanpa kehilangan data. Pemeriksaan integritas data menggunakan algoritma hash SHA-256 menunjukkan kecocokan 100% pada seluruh siklus backup, yang menegaskan keutuhan data cadangan.

Selain itu, pertumbuhan kebutuhan penyimpanan tercatat sebesar 2,8 TB, lebih

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

rendah dari estimasi awal sebesar 3,2 TB, yang menunjukkan efektivitas penerapan kompresi dan deduplikasi data. Dari sisi biaya, sistem yang dikembangkan membutuhkan anggaran sekitar Rp7,2 juta per tahun, jauh lebih rendah dibandingkan solusi komersial sejenis yang umumnya memerlukan biaya lebih dari Rp20 juta per tahun. Temuan ini menunjukkan bahwa sistem mampu memberikan efisiensi biaya yang signifikan tanpa mengorbankan kualitas layanan.

2. Hasil Pengujian Recovery

Pengujian recovery dilakukan secara komprehensif untuk menilai kemampuan sistem dalam memenuhi target pemulihan yang telah ditetapkan. Hasil pengujian menunjukkan bahwa seluruh skenario pemulihan berhasil memenuhi target Recovery Time Objective (RTO) dan Recovery Point Objective (RPO). Rincian pencapaian RTO dan RPO disajikan pada Tabel 4, yang memperlihatkan konsistensi sistem dalam memulihkan data dan layanan sesuai dengan batas toleransi yang direncanakan.

Skenario	RTO Traget	RTO Aktual	% Achievement	RPO target	RPO Aktual	% Achievement
Full Server Failure	<4 jam	1:48	55% lebih cepat	<1 jam	30 menit	50% lebih baik
Ransomware mock attack	<4 jam	1:55	52% lebih cepat	<1 jam	20 menit	67% lebih baik
Power Outage + Disk Fail	<4 jam	2:02	49% lebih cepat	<1 jam	35 menit	42% lebih baik
Rata - rata	4:12	1:59	52% lebih cepat	1:24	38 menit	46% lebih baik

Gambar 3. Pencapaian RTO/RPO

3. Evaluasi terhadap Kriteria Keamanan Data

Evaluasi sistem terhadap kriteria keamanan data menunjukkan bahwa sistem backup dan recovery yang dikembangkan telah memenuhi seluruh prinsip CIA Triad, yaitu kerahasiaan, keutuhan, dan ketersediaan data. Kerahasiaan data dijaga melalui penerapan enkripsi dan kontrol akses, keutuhan data dipastikan melalui mekanisme verifikasi hash, dan ketersediaan data didukung oleh arsitektur hybrid serta mekanisme pemulihan yang andal. Tingkat kepatuhan sistem terhadap prinsip CIA Triad disajikan pada Tabel 5, yang menunjukkan bahwa seluruh aspek keamanan data telah terpenuhi secara optimal.

Pembahasan

Hasil penelitian menunjukkan bahwa penerapan sistem backup dan recovery berbasis arsitektur hybrid mampu menurunkan rata-rata waktu henti sistem (downtime) secara signifikan, dari sebelumnya sekitar tiga hari menjadi 1 jam 59 menit, atau berkurang sebesar 82%. Selain itu, mekanisme cloud fallback berhasil digunakan pada sekitar 30% skenario pengujian dengan tingkat keberhasilan mencapai 98%, yang menegaskan peran penting penyimpanan cloud dalam meningkatkan ketersediaan data saat terjadi gangguan pada infrastruktur lokal.

Jika dibandingkan dengan penelitian sebelumnya, hasil penelitian ini menunjukkan peningkatan kinerja yang signifikan. Dibandingkan dengan penelitian Arnomo (2019), tingkat keberhasilan backup meningkat dari 95% menjadi 97,8%. Sementara itu, dibandingkan dengan temuan Rosano (2020), waktu pemulihan sistem

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

berhasil dipercepat dari lebih dari dua jam menjadi 1 jam 59 menit. Inovasi utama penelitian ini terletak pada penerapan sistem backup dan recovery hybrid yang dirancang khusus untuk konteks UKM dengan keterbatasan sumber daya, bersifat cost-effective, serta selaras dengan regulasi nasional BSSN Tahun 2024.

Dari sisi implikasi praktis, penelitian ini menunjukkan bahwa UKM dapat menerapkan sistem keamanan data dengan standar setara enterprise tanpa harus menanggung beban biaya yang tinggi. Sistem yang dikembangkan juga meningkatkan ketahanan bisnis UKM terhadap ancaman lokal, khususnya risiko bencana alam di wilayah Sulawesi Selatan. Selain itu, sistem ini membantu UKM memenuhi ketentuan regulasi nasional terkait keamanan informasi tanpa menimbulkan tekanan finansial yang berlebihan. Model dan template sistem yang dihasilkan dalam penelitian ini berpotensi direplikasi dan diterapkan pada lebih dari 100 UKM di Kota Parepare maupun di daerah lain dengan karakteristik serupa.

Kesimpulan

Implementasi sistem backup–recovery hybrid menggunakan Bacula yang terintegrasi dengan penyimpanan NAS dan cloud berhasil mencapai seluruh target penelitian yang telah ditetapkan. Dari sisi kinerja teknis, sistem mampu memenuhi target Recovery Time Objective (RTO) sebesar 1 jam 48 menit dan Recovery Point Objective (RPO) sebesar 38 menit, dengan tingkat keberhasilan proses backup mencapai 97,8%. Selain itu, sistem telah memenuhi prinsip keamanan data CIA Triad serta dinyatakan selaras dengan ketentuan Peraturan BSSN Nomor 7 Tahun 2024.

Dari aspek efisiensi biaya, sistem yang dikembangkan menunjukkan tingkat cost-effectiveness yang tinggi dengan biaya operasional sekitar Rp7,2 juta per tahun, atau lebih hemat sekitar 75% dibandingkan solusi komersial sejenis. Sistem juga dinilai siap digunakan pada lingkungan produksi karena telah dilengkapi dengan dokumentasi teknis dan panduan implementasi yang komprehensif. Hasil penelitian ini membuktikan bahwa UKM dengan keterbatasan sumber daya tetap dapat mengimplementasikan sistem keamanan data berstandar enterprise melalui pendekatan hybrid yang tepat, khususnya pada konteks Kota Parepare yang memiliki keterbatasan infrastruktur internet dan tingkat risiko bencana alam yang relatif tinggi.

Saran

Pengembangan lanjutan disarankan untuk mengarah pada perluasan pemanfaatan sistem melalui model layanan berlangganan yang terjangkau serta integrasi dengan platform digital UKM, sehingga sistem dapat digunakan secara lebih luas dan berkelanjutan. Dari sisi kebijakan, diperlukan penguatan dukungan melalui kolaborasi dengan regulator dan pemerintah daerah dalam penyusunan pedoman teknis yang sederhana dan mudah diterapkan oleh UKM. Penelitian selanjutnya juga dapat difokuskan pada kajian jangka panjang, penerapan sistem di berbagai wilayah dan sektor usaha, serta pengembangan model penilaian risiko dan tingkat kematangan keamanan data yang sesuai dengan karakteristik UKM di Indonesia.

Pada tingkat implementasi, peningkatan kapasitas sumber daya manusia perlu dilakukan melalui program pelatihan praktis, sertifikasi dasar, serta pembentukan komunitas pengelola sistem backup bagi UKM. Simulasi pemulihan bencana disarankan untuk dilaksanakan secara berkala dengan skenario yang mendekati kondisi nyata dan didokumentasikan secara sistematis. Optimalisasi biaya dapat didukung melalui kerja sama antar-UKM, keterlibatan pemerintah daerah, serta penyediaan skema pembiayaan

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026

khusus. Dari sisi tata kelola dan pengembangan teknologi, sistem dapat ditingkatkan melalui integrasi kecerdasan buatan untuk deteksi dini gangguan, dukungan multi-cloud, penerapan lingkungan container dan mikroservis, serta penguatan keamanan melalui enkripsi lanjutan, penyimpanan backup yang tidak dapat diubah (immutable backup), dan arsitektur zero-trust sebagai tindak lanjut dari keberhasilan implementasi sistem dalam penelitian ini.

Daftar Pustaka

Arnomo, I. (2019). Simulasi Backup dan Restore Database Repository Institusi Menggunakan Software Bacula. JUST-IT UMJ, 7(2), 45-56.

Badan Nasional Penanggulangan Bencana (BNPB). (2024). Data Kejadian Bencana di Sulawesi Selatan Tahun 2024. Jakarta: BNPB.

Badan Siber dan Sandi Negara (BSSN). (2024). Peraturan BSSN No. 7 Tahun 2024 tentang Standar Keamanan Sistem Informasi. Jakarta: BSSN.

Badan Siber dan Sandi Negara (BSSN). (2024). Laporan Tahunan Keamanan Siber Indonesia 2024. Jakarta: BSSN.

Cybersecurity Ventures. (2025). Cybercrime Damages Report 2025. USA: Cybersecurity Ventures.

DCloud. (2024). RTO dan RPO dalam Disaster Recovery Plan. Diakses dari https://dcloud.co.id/blog/rto-dan-rpo-dalam-disaster-recovery-plan.html

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information Security Management Systems*. Geneva: ISO.

ITHB. (2023). Evaluasi Implementasi AOMEI Centralized Backupper pada Jaringan Komputer Kampus. Jurnal Teknologi Informasi, 15(3), 112-125.

National Institute of Standards and Technology (NIST). (2020). *NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems*. USA: NIST.

Prasetio, B.H. (2024). Village Data Backup and Disaster Recovery: A Comparative Study. JITECS UB, 12(1), 88-102.

PublikSultra. (2024). Perbedaan Full, Incremental, Differential Backup. Diakses dari https://publiksultra.id/perbedaan-full-backup-incremental-backup-dan-differential-backup-dalam-strategi-cadangan-data/

Rosano, A. (2020). Manajemen Backup Data untuk Penyelamatan Data Nasabah pada Sistem Perbankan. Jurnal REMIK Polgan, 5(3), 112-125.

Sainstech. (2019). Implementasi Sistem Backup Data Perusahaan Menggunakan Veeam Backup & Replication. Jurnal Sainstech ISTN, 8(2), 67-78.

ZettaGrid. (2023). Disaster Recovery Plan: Pengertian, Komponen, dan Pentingnya bagi Perusahaan. Diakses dari https://www.zettagrid.id/blog/2023/12/04/disaster-recovery-pengertian-drc-langkah-plan-dan-pentingnya-bagi-perusahaan/

Received: November 12, 2025 – Revised: November 22, 2025 - Accepted: Desember 18, 2025 - Published online: January 14, 2026