

Keandalan Metode Backup Data dalam *Business Continuity Plan*: Analisis *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*

Syifa Nurgaida Yutia^{1*}, Zuki Pristianoro Putro²

^{1*,2} Program Studi Teknologi Informasi, Fakultas Informatika, Universitas Telkom, Kabupaten Bandung, Provinsi Jawa Barat, Indonesia.

article info

Article history:

Received 14 February 2025

Received in revised form

20 March 2025

Accepted 1 May 2025

Available online October 2025.

Keywords:

Business Continuity Plan;

Backup Data; Electronic

Vaulting; Remote Journaling;

Database Shadowing;

MariaDB.

Kata Kunci:

Business Continuity Plan;

Backup Data; Electronic

Vaulting; Remote Journaling;

Database Shadowing;

MariaDB.

abstract

Data security and availability are crucial aspects of an organization's operational sustainability, particularly in addressing potential disruptions such as system failures, human errors, natural disasters, or cyberattacks. A Business Continuity Plan (BCP) is designed to ensure that critical business processes can continue operating despite incidents that threaten operations. One of the key elements of BCP is data backup strategies, which serve to maintain the integrity and availability of information within a system. This study explores the implementation of three primary data backup methods Electronic Vaulting, Remote Journaling, and Database Shadowing in a MariaDB database environment. The research employs an experimental approach, in which these three backup strategies are implemented within a MariaDB-based system. Electronic Vaulting is used for periodically backing up data to a secondary server to ensure data security in disaster recovery scenarios. Remote Journaling records transaction changes in near real-time, allowing data synchronization with a backup server without requiring full database storage at all times. Database Shadowing combines database replication and server fault tolerance mechanisms, ensuring that data is simultaneously updated across multiple locations. The implementation of these backup strategies is expected to enhance system resilience against disruptions and ensure the continuity of organizational operations in the event of data loss. This study provides insights for organizations in selecting and implementing data backup strategies that align with their Business Continuity Plan. Future research may explore the integration of encryption in data backups, additional security mechanisms such as multi-factor authentication, and the use of cloud backup services to enhance system flexibility and resilience.

abstract

Keamanan dan ketersediaan data merupakan aspek krusial dalam keberlangsungan operasional organisasi, terutama dalam menghadapi potensi gangguan seperti kegagalan sistem, kesalahan manusia, bencana alam, atau serangan siber. Business Continuity Plan (BCP) dirancang untuk memastikan bahwa proses bisnis yang vital dapat tetap berjalan meskipun terjadi insiden yang mengancam operasional. Salah satu elemen penting dalam BCP adalah strategi backup data, yang berfungsi untuk menjaga integritas dan ketersediaan informasi dalam sistem. Penelitian ini membahas implementasi tiga metode backup data utama, yaitu Electronic Vaulting, Remote Journaling, dan Database Shadowing, pada lingkungan basis data MariaDB. Metode penelitian dilakukan dengan pendekatan eksperimental, di mana ketiga strategi backup tersebut diimplementasikan dalam sistem berbasis MariaDB. Electronic Vaulting digunakan untuk mencadangkan data secara berkala ke server cadangan guna memastikan keamanan data dalam skenario pemulihan bencana. Remote Journaling diterapkan untuk mencatat perubahan transaksi secara hampir real-time, memungkinkan sinkronisasi data dengan server cadangan tanpa harus menyimpan keseluruhan basis data setiap saat. Database Shadowing mengombinasikan replikasi database dan mekanisme server fault tolerance, memastikan data dapat langsung diperbarui secara simultan di beberapa lokasi. Penerapan strategi backup ini diharapkan dapat meningkatkan ketahanan sistem terhadap gangguan serta memastikan keberlangsungan operasional organisasi dalam menghadapi risiko kehilangan data. Penelitian ini memberikan wawasan bagi organisasi dalam memilih dan mengimplementasikan strategi backup data yang sesuai dengan kebutuhan Business Continuity Plan mereka. Pengembangan lebih lanjut dapat dilakukan dengan mengeksplorasi penerapan enkripsi dalam backup data, penerapan mekanisme keamanan tambahan seperti multi-factor authentication, serta pemanfaatan layanan cloud backup untuk meningkatkan fleksibilitas dan ketahanan sistem.

Corresponding Author. Email: syifagaida@telkomuniversity.ac.id^{1}.

Copyright 2025 by the authors of this article. Published by Lembaga Otonom Lembaga Informasi dan Riset Indonesia (KITA INFO dan Riset). This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. 



ACM Computing Classification System (CCS)

EBSCOhost

Communication and Mass Media Complete (CMC)

1. Pendahuluan

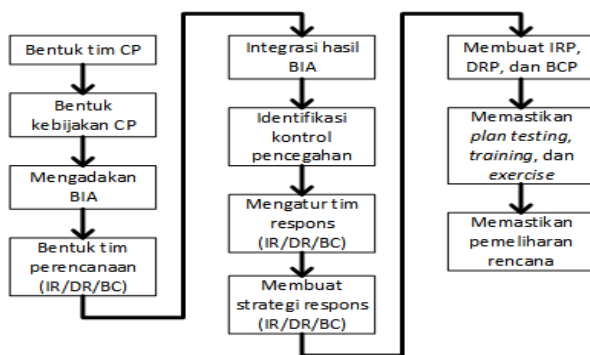
Data merupakan aset penting dalam operasional organisasi modern, terutama dalam lingkungan bisnis yang bergantung pada sistem informasi. Penyimpanan dan pengelolaan data yang efektif tidak hanya mendukung pengambilan keputusan yang lebih baik, tetapi juga memastikan kelangsungan operasional organisasi dalam menghadapi berbagai risiko yang dapat menyebabkan kehilangan atau kerusakan data (Salbiah & Nasution, 2024). Salah satu tujuan utama *Business Continuity Plan (BCP)* adalah untuk memastikan bahwa proses bisnis yang penting dapat pulih setelah gangguan (Zambon *et al.*, 2007). Risiko tersebut dapat berasal dari faktor internal seperti kesalahan manusia (*human error*) dan kegagalan sistem, maupun dari faktor eksternal seperti bencana alam dan serangan siber. Kehilangan data yang tidak ditangani secara tepat dapat berdampak signifikan terhadap efektivitas bisnis dan keberlanjutan operasional organisasi. Penerapan strategi *backup* data menjadi salah satu elemen penting dalam *BCP* untuk menjaga ketersediaan dan keamanan informasi. *BCP* merupakan serangkaian kebijakan dan prosedur yang dirancang untuk menjaga kelangsungan bisnis saat terjadi gangguan atau bencana (Mano *et al.*, 2012).

Salah satu aspek yang krusial dalam *BCP* adalah strategi *backup* data, yang bertujuan melindungi informasi organisasi melalui penyimpanan salinan data pada lokasi yang aman. Berbagai metode *backup* data telah dikembangkan untuk mengurangi potensi kehilangan data, antara lain *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*. *Electronic Vaulting* memungkinkan organisasi mentransfer data ke lokasi cadangan secara berkala sebagai langkah mitigasi risiko kehilangan. *Remote Journaling*, di sisi lain, menyediakan mekanisme pencatatan perubahan transaksi secara hampir *real-time* guna menjaga konsistensi data. Sementara itu, *Database Shadowing* menggabungkan sistem toleransi kesalahan server dengan mekanisme replikasi untuk meningkatkan redundansi dan ketersediaan data dalam skenario pemulihan bencana (Won *et al.*, 2019). Penelitian ini menerapkan dan mengevaluasi strategi *backup* data dalam *Business Continuity Plan* pada Aplikasi Manajemen Surat. Aplikasi tersebut digunakan untuk pengelolaan administrasi dan arsip dokumen

organisasi, sehingga membutuhkan sistem penyimpanan yang aman dan andal. Dengan mempertimbangkan pentingnya keberlanjutan operasional, penelitian ini bertujuan mengimplementasikan strategi *backup* data menggunakan metode *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing* pada sistem basis data *MariaDB*, serta menganalisis efektivitas masing-masing metode dalam menjaga integritas dan ketersediaan data. Evaluasi dilakukan untuk menilai sejauh mana keandalan sistem *backup* yang diterapkan dalam mendukung *Business Continuity Plan* organisasi. Hasil penelitian diharapkan menjadi dasar dalam menentukan strategi *backup* data yang tepat dan memperkuat ketahanan sistem informasi terhadap ancaman yang dapat mengganggu keberlangsungan layanan digital. Beberapa penelitian sebelumnya telah membahas penerapan strategi *backup* data dalam *Business Continuity Plan (BCP)*. Salah satu temuan menyatakan bahwa kombinasi antara *electronic vaulting* dan *database shadowing* dapat menurunkan waktu pemulihan data hingga 50% dibandingkan dengan metode *backup* konvensional (Won *et al.*, 2019). Berdasarkan telaah literatur tersebut, penelitian ini bertujuan mengevaluasi dan menerapkan strategi *backup* data menggunakan *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing* pada sistem basis data *MariaDB*. Pendekatan ini diharapkan menghasilkan solusi yang optimal dalam mendukung implementasi *BCP* secara lebih efektif dan efisien.

Contingency Planning atau perencanaan kontingensi merupakan proses menyeluruh yang bertujuan mempersiapkan organisasi dalam menghadapi kejadian tidak terduga. Tujuan utamanya adalah mengembalikan operasi ke kondisi normal dengan mengurangi biaya dan gangguan terhadap aktivitas bisnis setelah terjadinya insiden. Mengacu pada standar ISO 22301 (Pinto *et al.*, 2022; Haufe *et al.*, 2024), terdapat empat komponen utama dalam *CP*, yaitu *Business Impact Analysis (BLA)*, *Incident Response Plan (IRP)*, *Disaster Recovery Plan (DRP)*, dan *Business Continuity Plan (BCP)*. *BLA* merupakan langkah awal dalam *CP* yang digunakan untuk mengidentifikasi proses bisnis dan sistem informasi yang paling penting bagi keberhasilan organisasi. *IRP* berfokus pada respons awal yang dilakukan segera setelah insiden terjadi. Setiap kejadian merugikan yang tidak terduga dikategorikan sebagai insiden, dan tim respons insiden

dapat menyatakannya sebagai bencana (*disaster*). *DRP* bertujuan untuk memulihkan operasional bisnis di lokasi utama pascabencana. Apabila pemulihan di lokasi utama tidak memungkinkan dalam waktu singkat, maka *BCP* dijalankan bersamaan dengan *DRP*. *BCP* menekankan pada pelaksanaan operasi bisnis di lokasi alternatif hingga operasional dapat dikembalikan ke lokasi utama. Secara umum, *CP* memiliki siklus hidup sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. *Contingency Planning*

Business Continuity Plan (BCP) merupakan pendekatan strategis yang dirancang untuk menjaga kelangsungan operasional organisasi ketika terjadi gangguan yang dapat menghambat jalannya proses bisnis. Dalam situasi di mana lokasi utama tidak dapat digunakan akibat bencana, *BCP* memungkinkan proses-proses penting tetap dilaksanakan di lokasi alternatif. Rencana ini terdiri atas kebijakan dan prosedur yang bertujuan untuk meminimalkan dampak gangguan terhadap kegiatan bisnis serta mempercepat proses pemulihan pascainsiden (Dey, 2011; Monica *et al.*, 2020). Dalam implementasinya, strategi *backup* data menjadi salah satu komponen kunci dalam *BCP* karena berperan dalam menjaga integritas dan ketersediaan informasi penting bagi organisasi. Terdapat beberapa jenis fasilitas yang umum digunakan dalam mendukung *BCP*, seperti *hot site*, *warm site*, dan *cold site*, yang masing-masing berbeda dalam tingkat kesiapan dan biaya operasional. Selain itu, beberapa organisasi juga mengandalkan pendekatan bersama melalui *timeshare*, *service bureau*, atau *mutual agreement*, serta opsi fleksibel seperti *mobile site* yang dapat disesuaikan dengan kebutuhan lokasi dan mobilisasi. Salah satu strategi utama dalam perencanaan keberlangsungan bisnis adalah penerapan metode pencadangan data atau *backup*.

Proses ini melibatkan pembuatan salinan informasi digital untuk mencegah hilangnya data akibat kerusakan sistem, gangguan perangkat keras, maupun serangan siber. Dalam perancangannya, strategi *backup* harus mempertimbangkan frekuensi pencadangan, lokasi penyimpanan, serta metode pemulihan yang digunakan (Suguna & Suhasini, 2014). Beberapa metode yang sering diadopsi dalam industri mencakup *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*. *Electronic Vaulting* adalah metode pencadangan yang dilakukan dengan mentransfer data dari sistem utama ke lokasi penyimpanan eksternal melalui jaringan. Teknik ini sering digunakan dalam skenario *disaster recovery* karena memungkinkan data tetap tersedia meskipun sistem utama mengalami kerusakan. Umumnya, metode ini dipilih oleh organisasi yang membutuhkan tingkat keamanan tinggi dan akses data yang cepat. Berbeda dengan *electronic vaulting*, *remote journaling* hanya mentransfer data transaksi, bukan seluruh basis data, dan dilakukan hampir secara *real-time*. Pendekatan ini memungkinkan sinkronisasi yang cepat antara server utama dan server cadangan, sehingga perubahan transaksi dapat segera dicerminkan pada sistem cadangan.

Sementara itu, *database shadowing* merupakan bentuk lanjutan dari *remote journaling* yang menggabungkan teknik replikasi dengan sistem toleransi kesalahan server (*server fault tolerance*). Pendekatan ini memungkinkan pencadangan secara simultan di berbagai lokasi dengan memanfaatkan teknologi *mirroring*, sehingga jika server utama mengalami kerusakan, sistem dapat segera beralih ke cadangan tanpa kehilangan data. Hal ini menjadikan *database shadowing* sebagai salah satu metode dengan tingkat keandalan tinggi dalam memastikan keberlangsungan data dan layanan. Untuk mendukung implementasi ketiga metode tersebut, sistem manajemen basis data yang digunakan harus memiliki fleksibilitas dan kapabilitas teknis yang memadai. *MariaDB* merupakan salah satu platform *Relational Database Management System (RDBMS)* yang banyak digunakan sebagai alternatif dari *MySQL*. Platform ini memiliki keunggulan dalam hal performa, keamanan, serta fleksibilitas konfigurasi strategi pencadangan (Pina *et al.*, 2022). *MariaDB* mendukung berbagai metode pencadangan seperti *full backup*, *incremental backup*, *differential backup*, serta *master-slave replication*, yang kesemuanya memungkinkan integrasi dengan strategi

Electronic Vaulting, *Remote Journaling*, dan *Database Shadowing* secara optimal dalam mendukung *Business Continuity Plan* organisasi.

2. Metodologi Penelitian

Penelitian ini menggunakan pendekatan eksperimental yang bertujuan untuk mengimplementasikan dan mengevaluasi strategi *backup* data dalam mendukung *Business Continuity Plan* (BCP) pada sistem Aplikasi Manajemen Surat. Eksperimen dilaksanakan melalui penerapan tiga metode utama pencadangan data, yaitu *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*. Setiap metode diuji untuk menilai efektivitasnya dalam menjaga integritas serta ketersediaan informasi yang tersimpan pada sistem basis data. Evaluasi dilakukan secara menyeluruh untuk mengukur sejauh mana ketiga metode tersebut mampu memperkuat ketahanan sistem terhadap gangguan operasional. Implementasi sistem *backup* dilakukan pada infrastruktur berbasis *MariaDB*, yang telah dikonfigurasi agar mendukung ketiga strategi utama pencadangan. Untuk metode *Electronic Vaulting*, digunakan mekanisme *mysqldump* guna menyalin seluruh isi basis data dari server utama ke server cadangan dalam rentang waktu tertentu secara berkala. Metode *Remote Journaling* memanfaatkan fitur *binary log replication* pada *MariaDB*, yang memungkinkan setiap perubahan transaksi dikirim secara *real-time* ke server cadangan tanpa perlu mentransfer keseluruhan basis data. Sementara itu, *Database Shadowing* diterapkan melalui skema *master-slave replication* yang melibatkan lebih dari satu server cadangan, sehingga setiap pembaruan data yang terjadi pada server utama akan secara otomatis direplikasi secara simultan ke seluruh server cadangan.

3. Hasil dan Pembahasan

Hasil Implementasi

Pada tahap implementasi metode *Electronic Vaulting*, diperlukan dua unit server yang masing-masing berperan sebagai server utama (server basis data) dan server cadangan (*backup* server). Server cadangan

difungsikan untuk menerima serta menyimpan arsip data dalam bentuk file hasil dari proses *mysqldump*. Proses pencadangan ini dilakukan secara terjadwal dan terotomatisasi, dengan konfigurasi yang memastikan data dapat ditransfer secara aman ke server tujuan serta disimpan dalam format terkompresi guna menghemat ruang penyimpanan.

Tabel 1. Kebutuhan Server pada *Electronic Vaulting*

	Server Database	Server Backup
IP Address	192.168.1.10	192.168.1.21
OS	Debian 9	Debian 9
Database	MariaDB	-

Electronic Vaulting diterapkan dengan mengonfigurasi server basis data agar secara otomatis melakukan pencadangan dan mengirimkan salinan data ke server cadangan. Proses ini diawali dengan pembuatan direktori khusus untuk penyimpanan hasil pencadangan. Selanjutnya, sebuah *shell script* disusun untuk melakukan pencadangan basis data menggunakan utilitas *mysqldump*, kemudian file hasil pencadangan dikompresi dengan *gzip* dan disimpan pada direktori yang telah disiapkan. Penjadwalan pencadangan dilakukan secara otomatis menggunakan *cron job* yang dijalankan setiap pukul 03.00. Agar proses transfer data ke server cadangan berjalan efisien, konfigurasi *SSH key* diterapkan untuk memungkinkan akses tanpa memerlukan kata sandi. File hasil pencadangan kemudian dikirim ke server cadangan menggunakan protokol *SCP*, dan setelah proses transfer selesai, file tersebut dihapus dari server basis data utama guna mengoptimalkan ruang penyimpanan. Rangkaian konfigurasi ini dirancang untuk memastikan proses pencadangan berjalan secara otomatis, efisien, dan aman, sehingga potensi kehilangan data dapat diminimalkan.

Electronic Vaulting diterapkan dengan mengonfigurasi server basis data agar secara otomatis melakukan pencadangan dan mengirimkan salinan data ke server cadangan. Proses ini diawali dengan pembuatan direktori khusus untuk penyimpanan hasil pencadangan. Selanjutnya, sebuah *shell script* disusun untuk melakukan pencadangan basis data menggunakan utilitas *mysqldump*, kemudian file hasil pencadangan dikompresi dengan *gzip* dan disimpan pada direktori yang telah disiapkan. Penjadwalan pencadangan dilakukan secara otomatis menggunakan

cron job yang dijalankan setiap pukul 03.00. Agar proses transfer data ke server cadangan berjalan efisien, konfigurasi *SSH key* diterapkan untuk memungkinkan akses tanpa memerlukan kata sandi. File hasil pencadangan kemudian dikirim ke server cadangan menggunakan protokol *SCP*, dan setelah proses transfer selesai, file tersebut dihapus dari server basis data utama guna mengoptimalkan ruang penyimpanan. Rangkaian konfigurasi ini dirancang untuk memastikan proses pencadangan berjalan secara otomatis, efisien, dan aman, sehingga potensi kehilangan data dapat diminimalkan.

Remote Journaling

Pada implementasi *Remote Journaling*, diperlukan dua unit server yang terdiri atas satu server sebagai *master* dan satu server sebagai *slave*. Setiap server memiliki peran spesifik dalam proses replikasi data, di mana server *master* bertanggung jawab sebagai sumber utama data, sedangkan server *slave* berfungsi sebagai penerima data hasil replikasi. Konfigurasi ini memungkinkan pencatatan perubahan transaksi secara hampir real-time dari server *master* ke server *slave*, sehingga integritas dan ketersediaan data tetap terjaga. Adapun spesifikasi server yang digunakan untuk proses *Remote Journaling* disesuaikan agar mendukung kelancaran replikasi dan sinkronisasi data antara kedua server tersebut.

Tabel 2. Kebutuhan Server pada remote Journaling

	Server Master	Server Slave
IP Address	192.168.1.1	192.168.1.20
OS	Windows 10	Windows 10
Database	MariaDB	MariaDB

Tabel 3. Kebutuhan Server pada Data Shadowing

	Server Master	Server Slave 1	Server Slave 2	Server Slave 3
IP Address	192.168.1.1	192.168.1.20	192.168.1.21	192.168.1.22
OS	Windows 10	Windows 10	Windows 10	Windows 10
Database	MariaDB	MariaDB	MariaDB	MariaDB

Konfigurasi jaringan dan *MySQL* pada proses *data shadowing* dilakukan dengan menggunakan satu server *master* dan tiga server *slave* yang terhubung dalam jaringan *Local Area Network (LAN)*. Setiap server *slave* dikonfigurasi agar dapat berkomunikasi dengan server *master*, dengan pengaturan yang mencakup penyesuaian *IP Address* dan pembaruan konfigurasi *MySQL* untuk mengaktifkan fitur *log-bin* serta *server-id*

Langkah-langkah konfigurasi yang diperlukan untuk mengimplementasikan *Remote Journaling* dimulai dengan pengaturan jaringan dan *MySQL* pada server *master* dan *slave* untuk memastikan keduanya terhubung dalam jaringan *Local Area Network (LAN)*. Pengaturan *IP Address* dilakukan agar kedua server dapat saling berkomunikasi dengan baik. Selanjutnya, file konfigurasi *MySQL* diperbarui untuk mengaktifkan fitur *log-bin* dan *server-id*, kemudian layanan *Apache* dan *MySQL* dijalankan pada kedua server. Proses berikutnya adalah konfigurasi replikasi basis data, yang mencakup pemberian hak akses replikasi pada server *master* serta menghubungkan server *slave* ke server *master*. Setelah koneksi replikasi terbentuk, server *slave* akan secara otomatis menerima setiap perubahan data yang terjadi di server *master*. Tahap akhir adalah pengujian replikasi, yang dilakukan dengan melakukan berbagai operasi pada basis data di server *master*, seperti pembuatan basis data dan tabel, penambahan, pembaruan, serta penghapusan data, termasuk perubahan struktur tabel. Seluruh perubahan tersebut kemudian diverifikasi pada server *slave* untuk memastikan proses replikasi berjalan dengan baik dan data tersinkronisasi secara akurat.

Data Shadowing

Pada proses *data shadowing* diperlukan 4 (dua) unit server yang terdiri dari 1 (satu) server sebagai *server master* dan 3 (tiga) sebagai *server slave*. Berikut kebutuhan server untuk proses *data shadowing*.

pada setiap server. Selanjutnya, pada server *master* diberikan hak akses replikasi dan status *master* dicatat, sedangkan setiap server *slave* dikonfigurasi untuk terhubung dengan server *master* dan melakukan sinkronisasi data. Setelah seluruh konfigurasi selesai, status replikasi diperiksa guna memastikan proses berjalan tanpa kesalahan. Untuk memastikan keberhasilan replikasi, dilakukan berbagai operasi

pada basis data di server *master*, seperti pembuatan basis data dan tabel, penambahan, pembaruan, serta penghapusan data, termasuk perubahan struktur tabel. Setiap hasil operasi tersebut kemudian diverifikasi pada server *slave* untuk memastikan bahwa seluruh perubahan telah tersinkronisasi dengan benar.

Pembahasan

Implementasi strategi *backup* data dalam *Business Continuity Plan (BCP)* untuk Sistem Manajemen Surat merupakan langkah krusial dalam memastikan kesinambungan operasional dan perlindungan data organisasi. Menurut Salbiah dan Nasution (2024), pengelolaan data yang baik dalam sistem informasi manajemen sangat berpengaruh terhadap efektivitas pengambilan keputusan dan kelangsungan bisnis, sehingga perlindungan data melalui mekanisme *backup* menjadi kebutuhan utama. Dalam penelitian ini, tiga metode utama, yaitu *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*, telah diimplementasikan dan dievaluasi. Ketiga metode ini selaras dengan rekomendasi dari Zambon *et al.* (2007) yang menekankan pentingnya penggunaan model berlapis dalam *business continuity auditing* dan perencanaan pada sistem informasi. *Electronic Vaulting* menawarkan solusi pencadangan berkala yang dapat diotomatisasi menggunakan *mysqldump* dan *cron*, sehingga data secara rutin tersimpan di server cadangan. Namun, seperti yang diungkapkan Suguna dan Suhasini (2014), metode ini masih memiliki risiko kehilangan data pada interval pencadangan.

Sementara itu, *Remote Journaling* memungkinkan pencatatan transaksi secara *real-time*, sehingga setiap perubahan pada server utama langsung tersinkronisasi ke server cadangan. Hal ini sangat penting untuk menurunkan risiko *data loss* dan meningkatkan kecepatan pemulihan, sesuai dengan konsep *high availability* yang diuraikan oleh Won *et al.* (2019) dalam penelitian tentang sistem basis data terdistribusi. Namun, implementasi *Remote Journaling* memerlukan sumber daya jaringan dan konfigurasi sistem yang lebih kompleks. Metode *Database Shadowing* memberikan keunggulan dalam hal *fault tolerance* dan replikasi data secara menyeluruh ke beberapa node. Sistem dapat menjaga ketersediaan data dan mempercepat proses pemulihan saat terjadi

kegagalan, sejalan dengan model *Business Continuity Management* yang dikemukakan oleh Haufe *et al.* (2024). Penerapan *Database Shadowing* juga mendukung pembelajaran pencegahan bencana sebagaimana disarankan oleh Mano *et al.* (2012) melalui sistem pendukung *business continuity*. Dari hasil evaluasi, ketiga metode backup yang diimplementasikan pada MariaDB menunjukkan peningkatan signifikan dalam hal kecepatan pemulihan (*recovery time*), pengurangan risiko kehilangan data, dan peningkatan keandalan sistem terhadap potensi gangguan atau bencana. MariaDB dipilih karena fleksibilitas dan kemampuannya dalam mendukung berbagai skenario backup serta kompatibilitas dengan kebutuhan organisasi modern, sebagaimana dinyatakan oleh Pina *et al.* (2022) dalam studi perbandingan database *NewSQL*. Namun demikian, aspek keamanan data dalam proses *backup* dan pemulihan masih menjadi tantangan utama. Dey (2011) menegaskan bahwa perlindungan data harus mencakup enkripsi dan kontrol akses yang ketat untuk mencegah ancaman siber selama proses backup. Oleh karena itu, pengembangan selanjutnya dapat difokuskan pada penerapan enkripsi data sebelum backup serta penggunaan *multi-factor authentication (MFA)* untuk pengelolaan akses ke server backup, sebagaimana juga direkomendasikan dalam literatur terkait *business continuity* dan keamanan informasi. Hasil penelitian ini memperkuat temuan sebelumnya bahwa strategi backup yang tepat sangat penting untuk menjaga kontinuitas bisnis dan perlindungan data organisasi. Pemilihan metode backup harus mempertimbangkan kebutuhan spesifik organisasi, tingkat risiko, serta sumber daya yang tersedia. Dengan integrasi aspek teknis, manajerial, dan keamanan, organisasi dapat membangun sistem manajemen backup yang tangguh dan adaptif terhadap berbagai ancaman di masa depan.

4. Kesimpulan dan Saran

Penelitian ini telah berhasil mengimplementasikan dan mengevaluasi strategi *backup* data dalam *Business Continuity Plan (BCP)* untuk Sistem Manajemen Surat dengan menggunakan tiga metode utama, yaitu *Electronic Vaulting*, *Remote Journaling*, dan *Database Shadowing*. Hasil penelitian menunjukkan bahwa ketiga metode tersebut mampu meningkatkan keandalan

sistem, khususnya dalam menjaga integritas serta ketersediaan data. *Electronic Vaulting* diterapkan menggunakan *mysqldump* dan *cron*, yang memungkinkan proses pencadangan berkala ke server cadangan sehingga keamanan data tetap terjamin dalam skenario pemulihan bencana. Sementara itu, *Remote Journaling* menyediakan mekanisme pencatatan transaksi secara *real-time*, sehingga setiap perubahan pada server utama dapat langsung tersinkronisasi dengan server cadangan tanpa perlu menyimpan keseluruhan basis data secara berkala. Di sisi lain, *Database Shadowing* mengombinasikan toleransi kesalahan (*fault tolerance*) pada server dan replikasi basis data dalam skala lebih besar, sehingga proses pemulihan data dapat berlangsung lebih cepat ketika terjadi kegagalan sistem.

Dari hasil evaluasi, ketiga metode tersebut terbukti mampu meningkatkan kecepatan pemulihan data (*recovery time*), mengurangi risiko kehilangan data (*data loss*), serta meningkatkan keandalan sistem dalam menghadapi berbagai potensi gangguan atau bencana. Implementasi *backup* berbasis *MariaDB* juga memberikan fleksibilitas tinggi dalam pengelolaan maupun pemulihan data, sehingga menjadi pilihan yang tepat untuk mendukung *Business Continuity Plan* organisasi. Dapat disimpulkan bahwa penerapan strategi *backup* data yang tepat tidak hanya meningkatkan ketahanan data terhadap gangguan, tetapi juga secara signifikan mendukung kelangsungan operasional bisnis. Berdasarkan hasil penelitian ini, terdapat beberapa aspek yang dapat dikembangkan lebih lanjut untuk meningkatkan efektivitas strategi *backup* data dalam *Business Continuity Plan*. Salah satunya adalah eksplorasi penggunaan basis data alternatif, seperti *PostgreSQL*, *MySQL*, atau *NoSQL database*, guna membandingkan efektivitas dan kinerja sistem dalam berbagai skenario operasional. Selain itu, aspek keamanan data dalam proses *backup* perlu diperkuat dengan menerapkan enkripsi data sebelum pencadangan, agar informasi yang tersimpan lebih terlindungi dari ancaman siber. Penggunaan *multi-factor authentication (MFA)* dalam pengelolaan akses ke server *backup* juga penting untuk memastikan bahwa hanya pihak yang berwenang yang dapat melakukan perubahan atau pemulihan data.

5. Ucapan Terima Kasih

Penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada Departemen Penelitian dan Pengabdian Masyarakat Universitas Telkom Jakarta atas dukungan dananya melalui hibah publikasi. Dukungan ini sangat berperan dalam penyelesaian penelitian ini.

6. Daftar Pustaka

- Adeh, R., Ejila, I. O., & Olaniyi, A. R. (2020). Analysis of Current Models of Preservation of E-Resources in Nigerian Libraries.
- Andi, A., Wijaya, G., & Haeruddin, H. (2024, November). Implementasi Backup Solution berbasis Cloud untuk Mendukung Keandalan VPN Server pada PT Weefer Indonesia. In *National Conference for Community Service Project (NaCosPro)* (Vol. 6, No. 1, pp. 713-719). <https://doi.org/10.37253/nacospro.v6i1.9704>
- Buaty, N., Dutasmara, R., & Purwaningsih, M. (2024, December). Rancangan Business Continuity Planning (BCP) Perlindungan Data untuk Bank. In *Prosiding Seminar Nasional* (Vol. 4, pp. 66-75).
- Dey, M. (2011, February). Business continuity planning (BCP) methodology—Essential for every business. In *2011 IEEE GCC Conference and Exhibition (GCC)* (pp. 229–232). IEEE. <https://doi.org/10.1109/IEEEGCC.2011.5752503>.
- Haufe, K., Arias-Aranda, D., Dzombeta, S., & Stantchev, V. (2024). Business continuity management – a process reference model. <https://doi.org/10.2139/ssrn.4948959>.
- Mano, K., Inomo, H., Shiraki, W., & Isouchi, C. (2012, June). A business continuity plan support system for disaster prevention learning. In *2012 International Conference on Information Technology Based Higher Education and Training (ITHET)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ITHET.2012.6246073>.

- Mas' ud, I., & Salsabila, R. (2021). Perancangan business continuity plan pada PT. XYZ. *Jurnal Sistem Informasi dan Sains Teknologi*, 3(1), 492150. <https://doi.org/10.31326/sistek.v3i1.803>.
- Monica, R., Henry, Q., Estela, M., & Washington, F. (2020, June). Why implement continuity plans in organizations? Approach of a prospective study based on ITIL. In *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ISCV49265.2020.9204335>.
- Pina, E., Sá, F., & Bernardino, J. (2022). NewSQL databases assessment: CockroachDB, MariaDB Xpand, and VoltDB. *Future Internet*, 15(1), 10. <https://doi.org/10.3390/fi15010010>.
- Pinto, D., Fernandes, A., da Silva, M. M., & Pereira, R. (2022). Maturity models for business continuity—A systematic literature review. *Maturity models for business continuity—A systematic literature review*, (1), 123-136. <https://doi.org/10.18280/ijssse.120115>.
- Prakasita, E. H., & Ginardi, R. H. (2018). Tinjauan Kesiapan Terhadap Implementasi Business Continuity Management Systems (BCMS) Berbasis ISO 22301 DAN ISO 27001 (Studi Kasus: PT. JPK). *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 13.
- Salbiah, S., & Nasution, M. I. P. (2024). Analysis Of Data Processing In Management Information Systems. *Jurnal Ilmiah Ekonomi Dan Manajemen*, 2(12), 01-12. <https://doi.org/10.61722/jiem.v2i11.3017>.
- Suguna, S., & Suhasini, A. (2014, February). Overview of data backup and disaster recovery in cloud. In *International Conference on Information Communication and Embedded Systems (ICICES2014)* (pp. 1–7). IEEE. <https://doi.org/10.1109/ICICES.2014.7033804>.
- Won, Y., Kim, S., Yun, J., Tuan, D. Q., & Seo, J. (2019). DASH. *Proceedings of the VLDB Endowment*, 12(7), 793–806. <https://doi.org/10.14778/3317315.3317321>.
- Zambon, E., Bolzoni, D., Etalle, S., & Salvato, M. (2007, July). A model supporting business continuity auditing and planning in information systems. In *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)* (pp. 33-33). IEEE.