Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940

Pengamanan Backup dan Restore Basis Data dengan Penambahan Enkripsi Advanced Encryption Standard (Studi Kasus: Analisis Jabatan Bagian Organisasi Kabupaten Balangan)

Bambang Abdi Setiawan[1], Nur Hamid Sutanto[1,*], Gusti F Rahman[1], Ema Utami[1], M Syukri Mustafa[2]

[1] Magister Teknik Informatika, Universitas AMIKOM Yogyakarta, Sleman, Indonesia
[2] Teknik Informatika, STMIK Dipanegara, Makassar, Indonesia
Email: [1]frozenade@gmail.com, [2,*]hamid.alsa@gmail.com, [3]gt.rahman84@gmail.com, [4]ema_u@amikom.ac.id, [5]syukri@dipanegara.ac.id
Submitted: **20/03/2021**; Accepted:**28/04/2021**; Published: **30/05/2021**

Abstrak–Analisis jabatan diperlukan untuk menganalisis dan mendesain pekerjaan apa saja yang harus dikerjakan, bagaimana mengerjakannya, dan mengapa pekerjaan itu harus dilakukan. Analisis jabatan akan memberikan informasi mengenai uraian pekerjaan, spesifikasi pekerjaan, dan evaluasi pekerjaan bahkan dapat memperkirakan pengayaan atau perluasan pekerjaan dan penyederhanaan pekerjaan pada masa yang akan datang. Penelitian ini bertujuan untuk menerapkan prosedur manajemen pengamanan database sebagai langkah pencegahan kerusakan (error), kehilangan, dan pencurian data melalui metode backup dan restore yang disertai dengan enkripsi pada aplikasi Sistem Analisis Jabatan Bagian Organisasi Kabupaten Balangan (Simanja). Proses backup dengan menambahkan enkripsi Advanced Encryption Standard (AES) yang disimpan ke remote cloud hosting sebagai backup server menggunakan SSH Transfer Protocol (SFTP) memberikan keamanan yang memadai dan efisien. Hasil penelitian ini menunjukkan bahwa data yang disimpan di dalam database harus memiliki fitur atau fasilitas backup dan restore data dengan didukung oleh enkripsi sehingga data yang telah dicadangkan tersebut tetap aman tersimpan di media penyimpanan yang berada di luar media penyimpanan utama.

Kata Kunci: Backup; Restore; Database; SFTP; AES

Abstract–Job analysis is needed to analyze and design what work to do, how to do it, and why the work should be done. Job analysis will provide information about job descriptions, job specifications, and job evaluations and can even predict job enrichment or expansion and job simplification in the future. This study aims to implement database security management procedures as a measure to prevent damage (error), loss and theft of data through backup and restore methods accompanied by encryption in the Job Analysis System application of the Balangan Regency Organization Division (Simanja). The backup process by adding Advanced Encryption Standard (AES) encryption which is stored to remote cloud hosting as a backup server using SSH Transfer Protocol (SFTP) provides adequate and efficient security.

Keywords: Backup; Restore; Database; SFTP; AES

1. PENDAHULUAN

Dalam perkembangan teknologi informasi digital, data merupakan bagian penting bagi sistem informasi. Data yang tersimpan dapat dimanfaatkan kembali walaupun sudah lama tidak digunakan[1]. Karena itulah manajemen penyimpanan data dalam tempat penyimpanan (storage) harus menjadi perhatian.

Dalam database tersimpan data yang dimanfaatkan dalam rangka menjalankan proses bisnis suatu perusahaan atau organisasi. Dalam penyimpanan data ada potensi data yang rusak atau bahkan hilang yang disebabkan karena beberapa faktor, seperti malfungsi, mati listrik, kerusakan hardware, vandalisme, dan sebagainya. Data yang disimpan memiliki potensi ancaman yang bisa berasal dari faktor eksternal maupun internal. Faktor eksternal dapat berasal dari ancaman bencana alam maupun bencana non alam. Seperti banjir, gempa, kebakaran, dan lainnya yang menyebabkan tempat penyimpanan rusak dan data menjadi hilang. Sedangkan faktor internal dapat berasal dari kesalahan yang berasal dari pengembang atau pengelola data yang tidak melakukan langkah-langkah pencegahan kehilangan dan kerusakan data pada sistem[2].

Berdasarkan hal tersebut, dalam rangka melakukan antisipasi kemungkinan buruk yang mungkin terjadi, pengembang atau pengelola sistem penyimpanan data harus melakukan prosedur agar suatu sistem database mampu untuk mengembalikan data yang rusak maupun hilang setelah terjadi bencana[2]. Kemampuan yang dibuat untuk melakukan pencadangan (backup) dan kemampuan untuk melakukan pemulihan (restore) data.

Basis data memiliki kualitas berdasarkan skema database setidaknya meliputi 4 (empat) aspek, yaitu kebenaran (correctness), konsistensi (consistency), jangkauan (scope), dan minimalitas (minimality). Agar database yang disimpan tetap terjaga kualitasnya saat dibutuhkan, maka sistem informasi yang baik harus memiliki manajemen backup dan restore data yang baik dan aman[3].

Pada penelitian sebelumnya yang dilakukan tentang pengamanan data pada Aplikasi SIJALU di Universitas Semarang menjelaskan bahwa backup dan restore dilakukan menggunakan aplikasi remote connection yang diinstal di luar tempat penyimpanan dan data backup diletakkan di tempat penyimpanan cadangan yang terpisah yaitu cloud[4].

Sedangkan penelitian lainnya melakukan penelitian tentang keamanan data backup dan restore pada aplikasi DSpace yang mengacu pada CIA Triad, yaitu confidentiality dan availability dimana data yang di-backup

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940

dan kemudian di-restore adalah aman dan tidak mengalami perubahan sehingga ketika dilakukan proses restore, data yang dihasilkan sesuai dan sama dengan sebelum dilakukan backup[5].

Penelitian ini bertujuan untuk memberikan gambaran tentang manajemen pengamanan data terhadap database aplikasi Sistem Analisis Jabatan Bagian Organisasi Kabupaten Balangan (Simanja) menggunakan metode backup dan restore yang ditambah dengan enkripsi sebagai langkah pencegahan kerusakan (error), kehilangan, dan pencurian data.

Hasil dari penelitian ini menunjukkan bahwa dengan melakukan penambahan enkripsi Advanced Encryption Standard (AES) sebagai bentuk pengamanan data untuk backup, dimana hasil dari proses backup disimpan ke remote cloud hosting di server lain, memberikan keamanan yang memadai untuk aplikasi Simanja sehingga apabila terjadi kerusakan atau perubahan yang tidak diinginkan terhadap database, maka akan bisa dilakukan proses dekripsi dan restore sehingga aplikasi dapat digunakan kembali.

2. METODE PENELITIAN

2.1 Aplikasi Simanja

Sistem Analisis jabatan Bagian Organisasi Kabupaten Balangan yang disebut dengan Simanja merupakan aplikasi yang dikembangkan untuk mengumpulkan dan menganalisis semua informasi yang berkaitan dengan pekerjaan, antara lain: deskripsi, indikator, pendidikan dan kompetensi yang dibutuhkan, prosedur operasi melakukan pekerjaan, hasil pekerjaan serta kompensasi dan penilaian pekerjaan[3]. Sedangkan analisis jabatan menghasilkan informasi yang berharga bagi perusahaan atau instansi untuk penentuan strategi, seleksi, penilaian kinerja, pelatihan dan pengembangan profesi, desain dan redesain jabatan serta perencanaan SDM[6].

2.2 Backup Data

Backup merupakan suatu proses menyalin data yang sama di tempat yang berbeda. Fungsinya untuk mengantisipasi kejadian seperti kerusakan atau kehilangan data yang asli[7]. Hasil penyalinan data tersebut dikenal dengan sebutan “data backup”. Dengan kata lain, backup adalah kegiatan menyalin atau membuat file database cadangan, sehingga file database salinan atau cadangan tersebut disimpan dan dapat dipanggil kembali untuk mengganti file asli apabila terdapat kerusakan atau kehilangan. Backup bertujuan untuk menyalin data asli sebagai data cadangan yang disimpan di tempat yang berbeda dalam rangka mengantisipasi terjadinya kerusakan dan kehilangan data yang diakibatkan oleh bencana maupun kerusakan alat dan media penyimpanan utama.

2.3 Restore Data

Restore atau recovery adalah satu proses yang dilakukan untuk memanggil dan mengembalikan data yang dicadangkan dan disimpan melalui proses backup. Restore menjadi sebuah proses penting setelah backup. Proses restore tidak akan berhasil jika backup tidak dilakukan secara jelas dan prosedur yang terstruktur. Aplikasi restore atau recovery yang siap digunakan secara instan juga banyak ditemukan. Bahkan sudah dilengkapi dengan fitur backup otomatis. Fitur backup otomatis akan sangat membantu karena dapat memberikan kepastian proses backup yang terstruktur dengan baik dan teratur, serta memberikan kepastian keberhasilan dari proses restore[7].

2.4 Storage

Storage atau tempat penyimpanan adalah suatu tempat yang digunakan dalam menyimpan data atau file. Terkait data digital, storage merupakan tempat penyimpanan data cadangan yang dihasilkan dari proses backup. Dalam istilah teknologi informasi, storage identik dengan server. Dalam pengamanan data backup, media penyimpanan yang akan digunakan harus melalui proses pertimbangan, antara lain: keamanan, kapasitas, kemudahan akses informasi data, dan biaya. Storage direkomendasikan tidak berada di perangkat yang sama dengan data utama.
Tempat penyimpanan menjadi satu hal yang penting bagi sistem database. Karena yang selalu tersedia merupakan kebutuhan mutlak pada infrastruktur setiap organisasi. Ketika diperlukan, ketersediaan data yang disimpan harus dipastikan siap untuk diakses. Database merupakan suatu kumpulan data digital yang ketika disimpan memiliki tingkat risiko dan ancaman. Resiko dan ancaman tersebut salah satunya berasal dari storage, seperti kurangnya perawatan, database rusak, hardware media rusak, error data, kebakaran, serta bencana alam yang kejadiannya tidak terduga seperti banjir dan gempa bumi[7].
Cloud Storage dalam Bahasa Indonesia adalah penyimpanan awan. Cloud storage adalah suatu media penyimpanan yang menggunakan jaringan internet dalam melakukan akses terhadap file yang disimpan. Cloud storage merupakan penyimpanan yang hemat tempat, praktis dan hemat sumber daya, seperti penggunaan hardware dan konsumsi daya listrik[8].

2.5 Remote Backup Server

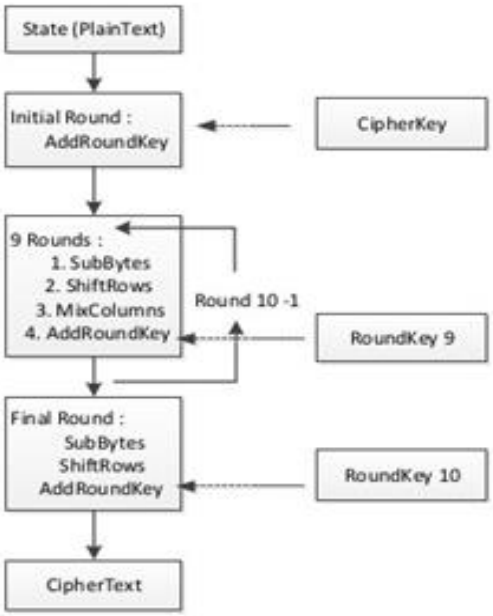
Remote Backup adalah cara melakukan proses backup data di storage yang berada di tempat lain secara jarak jauh. Metode remote backup banyak digunakan oleh perusahaan atau lembaga yang memiliki penyimpanan berupa server yang diletakkan di tempat yang berbeda dengan penyimpanan data utamanya.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940

Metode remote backup menggunakan teknik penyimpanan secara terkontrol terhadap cloud backup. Cara backup database menggunakan metode ini adalah dengan melakukan proses secara online yang dapat dilakukan kapan saja, dari mana saja, dan menggunakan device apa saja selama bisa terhubung ke internet menggunakan web browser. Remote backup memungkinkan proses backup dilakukan secara cepat dan realtime sesuai dengan waktu yang ditentukan, sedangkan proses restore database dilakukan pada saat dibutuhkan.
Cloud server muncul bermula dari metode remote backup yang mulai dikenal dan digunakan secara luas serta menjadi bagian penting dalam aktivitas bisnis. Bahkan tampilan antarmuka (GUI) yang dirancang untuk kemudahan pengguna[9]. Penggunaan piranti didukung aplikasi yang membutuhkan penyimpanan data oleh pengguna difasilitasi dengan penyimpanan lokal dan di-backup dengan penyimpanan cloud. Konsep server cadangan adalah tempat penyimpanan data yang terpisah dengan tempat penyimpanan utama, bisa jarak jauh atau menggunakan penyimpanan awan.
SSH File Transfer Protocol atau yang dikenal dengan SFTP memberikan jaminan terhadap keamanan transfer atau pemindahan file atau data. SFTP menggunakan protokol SSH dan mendukung pengenkripsian file dengan model keamanan sehingga menobatkannya sebagai FTP yang tergolong memiliki keamanan dan terhindar dari berbagai serangan dan ancaman saat proses transfer data[10]. Proses yang dilakukan SFTP yaitu memindahkan data atau file dengan menjadikan paket melalui satu jalur penghubung yang aman. SFTP menjadi salah satu protokol pilihan yang dapat digunakan dalam pemindahan data.

2.6 Advanced Encryption Standard (AES)

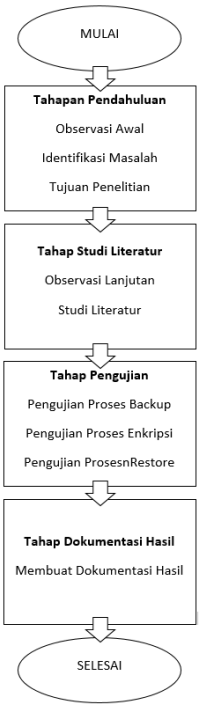
Algoritma kriptografi Advanced Encryption Standard (AES) merupakan standar algoritma enkripsi kunci simetris. Kriptografi adalah teknik untuk menjaga keamanan informasi dengan cara mengubah data menjadi bentuk tersandi yang tidak bisa dibaca[11]. Pihak yang berwenang dapat membaca data yang tersandi yaitu penerima atau pengirim pesan. Informasi atau pesan yang telah disamarkan disebut dengan ciphertext sedangkan pesan yang tidak disamarkan disebut dengan plaintext. Enkripsi merupakan cara penyamaran sebuah pesan yang asli menjadi tidak bisa terbaca, sedangkan proses untuk mengubah data kembali agar dapat terbaca disebut dengan dekripsi.
Kriptografi yang sudah tersandi harus didukung dengan algoritma yang baik dengan waktu dibutuhkan lebih banyak sehingga data menjadi lebih kuat dan aman. Algoritma kriptografi modern dibagi menjadi dua kategori, yaitu algoritma kunci simetrik dan kunci asimetrik. AES merupakan kategori algoritma kriptografi kunci simetrik yang sangat bagus dan juga sebagai algoritma cipher block dengan memanfaatkan teknik permutasi, substitusi dan sejumlah putaran pada setiap blok yang akan dienkripsi[12].
Algoritma AES memiliki empat jenis perubahan bytes, yaitu MixColumns, SubBytes, ShiftRows dan AddRoundKey. Pada proses enkripsi, input yang telah disalin ke state akan mengalami perubahan byte AddRoundKey. Kemudian state akan berubah menjadi MixColumns, SubBytes, ShiftRows dan AddRoundKey secara looping sebanyak Nr. Yang mana proses ini dikenal dengan round function. Pada round yang terakhir mengalami perubahan Mixcolumns. Adapun Proses enkripsi AES dapat dilihat pada Gambar 1.



Gambar 1. Proses Enkripsi AES

Penelitian ini menggunakan implementasi dan pengujian backup, restore, enkripsi dan remote backup terhadap database sesuai dengan prosedur pengamanan data untuk mencegah database mengalami kerusakan bahkan kehilangan. Alur penelitian yang dilakukan dapat dilihat pada Gambar 2.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940



Gambar 2. Alur Penelitian

Aplikasi Simanja dikembangkan dengan basis web sehingga setiap unit kerja yang terkait dapat mengakses aplikasi tersebut dengan mudah secara daring menggunakan peramban yang terhubung ke internet. Lokasi aplikasi beserta database-nya diletakkan pada cloud hosting dengan uptime mendekati 100 persen, sedangkan media penyimpanan untuk backup ditempatkan secara remote menggunakan SFTP pada cloud hosting yang berbeda. Proses backup dilakukan secara otomatis setiap hari pada pukul 03.00 pagi menggunakan cron job dan dapat diatur intervalnya sesuai kebutuhan. Dapat dilihat pada Gambar 3.

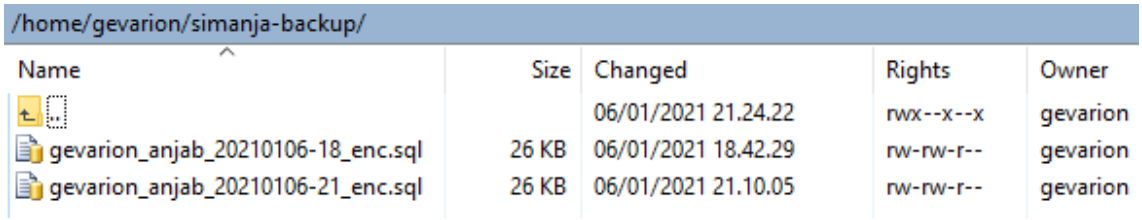
Gambar 3. Cron Job untuk Jadwal Backup

Sebelum disimpan ke remote cloud hosting, file backup ditambahkan enkripsi AES untuk menjamin keamanan basis data yang dikelola. Kata sandi ditentukan oleh operator pada pengaturan aplikasi sebelum proses backup dilakukan. Sedangkan apabila ingin dilakukan restore, operator cukup menarik file yang telah disimpan di remote cloud hosting untuk di-dekripsi. Selanjutnya file hasil dekripsi yang telah dihasilkan dalam bentuk SQL bisa diimpor setiap saat oleh operator ke dalam database menggunakan PHPMyAdmin apabila diperlukan.

3. HASIL DAN PEMBAHASAN

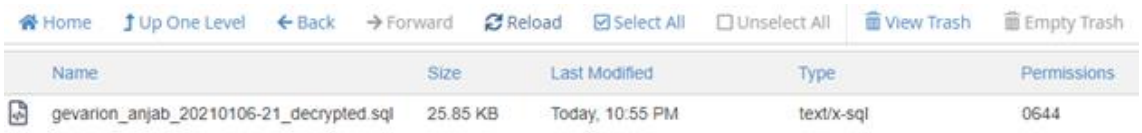
Uji coba dilakukan dengan menjalankan skrip backup database yang telah diatur sesuai jadwal pada cloud hosting aplikasi Simanja. Setelah proses selesai, file hasil backup yang telah di-enkripsi menggunakan AES akan tersimpan pada remote cloud hosting yang dituju menggunakan SFTP. Keberhasilan proses backup dapat dilihat pada Gambar 4.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940



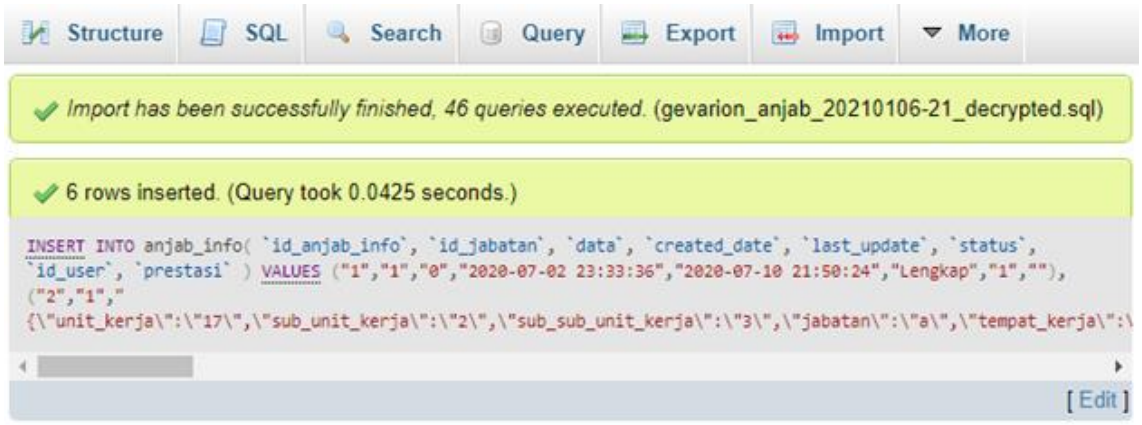
Gambar 4. File Backup pada Remote Cloud Hosting

Selanjutnya, dilakukan pengujian dengan menjalankan skrip dekripsi terhadap file backup yang tersimpan di remote cloud hosting lalu ditransfer ke cloud hosting dimana aplikasi dijalankan. Hasil file backup yang berhasil di-dekripsi dapat dilihat pada Gambar 5.



Gambar 5. File Hasil Dekripsi dari File Backup

Pengujian restore menggunakan teknik impor file SQL yang telah di-dekripsi ke dalam database aplikasi Simanja berhasil dilakukan. Dapat dilihat pada Gambar 6.



Gambar 6. Proses Restore Berhasil Dilakukan

Pengujian white-box menggunakan skrip PHP untuk melakukan backup menggunakan SFTP, enkripsi terhadap file backup, dekripsi terhadap file backup dan restore ke dalam database aplikasi SImanja menunjukkan keberhasilan mencapai 100%. Untuk lebih jelasnya dapat dilihat pada Tabel 1.

Tabel 1. Hasil Pengujian White-Box

No	Kasus Uji	Langkah Pengujian	Hasil
1	Melakukan backup database	MySQL database dump	File backup tercipta
2	Proteksi file backup	Enkripsi AES	FIle backup di-enkripsi
3	Connection server SFTP dengan SSH authentication	Remote connection server	Terhubung ke remote server
4	Penyimpanan file backup	File transfer ke remote server	File backup tersimpan
5	File backup transfer	Dekripsi file backup	File backup berhasil diimpor
6	Restore database	Impor database	Database berhasil diimpor

4. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa data yang disimpan di dalam database harus memiliki fitur atau fasilitas backup dan restore data dengan didukung oleh enkripsi sehingga data yang telah dicadangkan tersebut tetap aman tersimpan di media penyimpanan yang berada di luar media penyimpanan utama. Proses restore akan menjadi tidak berguna, jika proses sebelumnya tidak dipastikan berjalan dengan sesuai prosedur yang diharapkan. Keberhasilan proses backup dan enkripsi data, dilanjutkan dengan keberhasilan dekripsi dan restore data. Yang harus difinalisasi dalam penerapan sistem informasi database adalah berjalannya prosedur pelaksanaan backup

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 2, Nomor 3, Mei 2021
e-ISSN 2685-998X
DOI 10.30865/json.v2i3.2940

data yang terstruktur. Termasuk di dalamnya frekuensi backup yang bisa secara periodik, dan penentuan storage atau penyimpanan yang akan digunakan untuk menyimpan data backup. Sistem informasi yang berisi data penting, harus diamankan baik dari kerusakan, kehilangan, atau bahkan pencurian data. Untuk itu data selain di backup juga harus di-enkripsi dengan harapan mengantisipasi pencurian data. Data yang di enkripsi harus dipastikan aman dan dapat di dekripsi dengan hasil yang sama dengan data backup asli sebelum di enkripsi. Sehingga data backup memiliki kualitas data yang baik. Penelitian ini menunjukkan tingkat keberhasilan sebesar 100% setelah dilakukan pengujian backup dan restore database yang dilakukan secara remote dengan menambahkan enkripsi sesuai dengan alur penelitian yang telah direncanakan.

REFERENCES

[1] E. Wijaya, R. Robet, and R. Robin, "Perancangan Sistem Otomatisasi Backup Data Menggunakan File Transfer Protocol Berbasis Jaringan LAN (Studi Kasus Pada STMIK TIME Medan)," *J. TIMES*, vol. 4, no. 1, pp. 26–30, 2015, [Online]. Available: http://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/219.

[2] W. Chen and Y. T. Shang, "Disaster Recovery of Online System Based on Cloud Computing," *Appl. Mech. Mater.*, vol. 865, pp. 636–641, 2017, doi: 10.4028/www.scientific.net/amm.865.636.

[3] N. H. Sutanto, B. A. Setiawan, G. F. Rakhman, E. Utami, and M. S. Mustafa, "Jurnal Syntax Admiration," *J. Syntax Admiration*, vol. 1, no. 7, pp. 304–314, 2020.

[4] W. Adhiwibowo, M. S. Suprayogi, and A. Nugroho, "Pengamanan Data Pada Aplikasi Sijalu Universitas Semarang," *J. Pengemb. Rekayasa dan Teknol.*, vol. 14, no. 1, pp. 24–27, 2018.

[5] I. Arnomo, "Simulasi Backup Dan Restore Database Repository," *J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 9, no. 2, pp. 92–99, 2019.

[6] Wirawan, *Evaluasi Kinerja Sumber Daya Manusia: Teori, Aplikasi dan Penelitian*. Salemba Empat Jakarta, 2015.

[7] A. Rosano and D. Sudaradjat, "Manajemen Backup Data untuk Penyelamatan Data Nasabah pada Sistem Informasi Perbankan (Studi Kasus : PT Bank XYZ)," *REMIK (Riset dan E-Jurnal Manaj. Inform. Komputer)*, vol. 4, no. 2, p. 1, 2020, doi: 10.33395/remik.v4i2.10507.

[8] I. Santiko and R. Rosidi, "Pemanfaatan Private Cloud Storage Sebagai Media Penyimpanan Data E-Learning Pada Lembaga Pendidikan," *J. Tek. Inform.*, vol. 10, no. 2, pp. 137–146, 2018, doi: 10.15408/jti.v10i2.6992.

[9] M. Raje and D. Mukhopadhyay, "A Survey on Backup of Data on Remote Server," *Int. J. Sci. Res.*, vol. 3, no. 12, 2014.

[10] C. Ariata, "Cara Transfer File dengan Aman Menggunakan SFTP," *Hostinger*, 2020. https://www.hostinger.co.id/tutorial/transfer-file-dengan-sftp/#Apa-Itu-SFTP (accessed Jan. 06, 2021).

[11] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016, [Online]. Available: https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067.

[12] R. H. Dedi Kurniawan, Rita Afyenni, "Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan Cloud Storage Berbasis Android," *ISSN Media Elektron.*, vol. 3, no. September, pp. 4–5, 2018.