E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 3 No 7 Tahun 2024, Hal 100-111

STRUKTUR BASIS DATA DI ERA DIGITAL (IMPLEMENTASI PENGAMANAN BASIS DATA DI ERA GLOBAL)

[1]Khoiri Gusnanda, [2]Nur Ulfadillah, [3]Titin Sumarni
Email:khoirigusnanda3@gmail.com Ulfadillah85@gmail.com Titinijal@gmail.com
Program Studi Ekonomi Syariah Jurusan Syariah dan Ekonomi Islam
Sekolah Tinggi Agama Islam Negeri (STAIN) Bengkalis

Abstrak

Tulisan ini membahas pentingnya keamanan data dalam sistem informasi, khususnya pada sistem penjualan di era digital. Fokusnya adalah pada implementasi pengamanan basis data menggunakan teknik enkripsi MD5 dan teknologi blockchain. Artikel juga membahas teknologi database dalam pengelolaan data bisnis serta pemanfaatan blockchain untuk meningkatkan transparansi dan keamanan dalam berbagai sektor, termasuk keuangan dan kontrak. Implementasi teknologi Oracle Security Server juga dibahas sebagai bagian dari pengamanan basis data. Meskipun terdapat beberapa tantangan teknis dan infrastruktur, seperti skala jaringan terbatas dan ketersediaan SDM yang terbatas, teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan dan transparansi dalam transformasi digital di Indonesia.

Kata kunci: Struktur, Basis Data, Era Digital

A. Pendahuluan

Saat ini, dapat dikatakan hampir semua institusi swasta, pemerintah ataupun perusahaan telah menggunakan sistem informasi untuk dapat menghasilkan informasi yang digunakan oleh berbagai level manajemen. Berbagai istilah, seperti data, data base, informasi dan sistem informasi muncul. Aplikasi dalam organisasi, aplikasi client-server, aplikasi e-Commerce, aplikasi ebussines merupakan fungsi utama dari basis data. Tujuan basis data adalah membantu orang dan organisasi menelusuri hal-hal tertentu. Database (dan khususnya SQL) telah lama menjadi bagian integral dari sistem dalam menjalankan bisnis, baik dalam bentuk awalnya, yaitu file database biasa maupun dalam bentuk sekarang ini,yaitu database yang berorientasi pada tingkat lanjut. Kebutuhan atas penyimpanan dan pengaksesan informasi secara cepat menjadi hal-hal yang mendesak bagi tiap bisnis atau aplikasi, begitu pula web. [1]

Aplikasi-aplikasi web sekarang ini berpasangan dengan database. Database dipakai untuk beragam kegunaan mulai dari menyimpan nama-nama user dan password-pasword untuk akses resmi, sampai untuk menyimpan alamat-alamat email user, dan informasi kartu kredit untuk mempermudah pengiriman produk dan pembayarannya. Oleh karena itu, pemahaman menyeluruh mengenai keamanan web harus mencakup juga lapisan databasenya dan terpenting memahami juga bagaimana penyusup berusaha memasuki aplikasi untuk memperoleh akses ke bagian-bagian datanya**.**

B. Identifikasi Masalah

Keamanan dan kerahasian data pada Sistem penjualan sangat penting artinya, baik pada saat pengiriman ataupun pada saat data atau informasi tersebut diterima, karena data atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau

[1] Gatot Susilo, "Keamanan Basis Data Pada Sistem Informasi Di Era Global," *Jurnal TRANSFORMASI* 12, no. 2 (2016),hal.78–87.

berkepentingan, dari uraian di atas, maka dapat didefinisikan masalahnya sebagai berikut:

1. Diperlukan sebuah sistem untuk menangani masalah keamanan database
2. Belum adanya sistem penjualan yang menggunkan pengamanan database login user dengan menggunakan teknik Enkripsi Md5 dan blockhain

C. Metode

Identifikasi Topik dan Tujuan Penelitian Tahap pertama dalam penelitian ini adalah mengidentifikasi topik dan merumuskan tujuan penelitian. Peneliti menetapkan fokus penelitian pada pengaruh teknologi blockchain terhadap transparansi dan keandalan pelaporan keuangan. Tujuan penelitian adalah untuk mengeksplorasi bagaimana blockchain dapat meningkatkan kedua aspek tersebut dan untuk mengidentifikasi tantangan serta manfaat yang terkait dengan implementasinya. Pencarian Literatur Peneliti melakukan pencarian literatur yang relevan dengan topik penelitian menggunakan berbagai sumber akademik seperti jurnal, buku, konferensi, dan database online (misalnya, Google Scholar, IEEE Xplore, JSTOR, dan lainnya). Kata kunci yang digunakan dalam pencarian meliputi "blockchain", "financial reporting", "transparency", "reliability", "blockchain implementation", dan "financial audit".

D. Hasil Dan Pembahasan

1. Pengamanan Data

Menurut Herryawan secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Keamanan data biasanya terkait hal-hal berikut: Fisik, dalam hal ini pihak yang tidak berwenang terhadap data berusaha mendapatkan data dengan melakukan kegiatan sabotase atau penghancuran tempat penyimpanan data. Organisasi, dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menangani data tersebut. Ancaman dari luar, dalam hal ini pihak yang tidak berwenang berusaha untuk mendapatkan data melalui media komunikasi dan juga melakukan pencurian data yang tersimpan di dalam komputer.[2]

Dalam melakukan pengamanan data dibutuhkan sebuah teknik yang disebut dengan kriptografi. Kriptografi merupakan teknik untuk mengubah atau menyamarkan sebuah informasi sehingga informasi tersebut ketika ditransmisikan menjadi tidak dikenali atau tidak berupa sebuah informasi. Dalam kriptografi terdiri dari enkripsi dan dekripsi. Enkripsi adalah proses untuk pengubahan data menjadi data yang tidak berbentuk sebuah informasi dengan menggunakan algoritma tertentu. Dekripsi merupakan proses perubahan data yang telah di enkripsi ke dalam bentuk semula. Kriptografi banyak digunakan di dalam dunia digital karena tingkat keamanan datanya dapat mencegah *cyber-crime* menerobos sebuah sistem.[3]

Teknologi kriptografi sangat berperan penting dalam komponen komunikasi, untuk melakukan enkripsi/penyandian (pengacakan) data yang ditransmisikan

---

[2] Stmik Subang and Enkripsi Kriptografi Gost, "Pengamanan Basis Data Sistem Penjualan Dengan Menggunakan Teknik Enkripsi Kriptograsi Gost," *Jurnal Teknologi Informasi dan Komunikasi* 2, no. April (2018): 49–66.

[3] Kristovorus Zalukhu, Yohanni Syahra, and Trinanda Syahputra, "Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan," *J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)* 3, no. 2 (2020): 138.

selama pengiriman dari sumber ke tujuan dan juga melakukan dekripsi (pengembalian ke awal) data yang telah teracak tersebut. Sebuah data perlu dilakukan pengamanan untuk menjaga kerahasiaan data dan informasi penting. Yang sering digunakan untuk melakukan pengamanan data adalah kriptografi. Kriptografi adalah salah satu teknik yang berkaitan dengan keamanan data seperti kerahasiaan sebuah data, integritas data, serta otentikasi.[4]

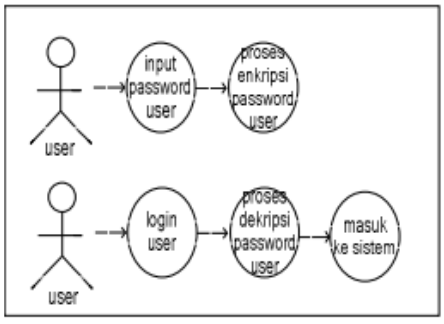
2. Definisi MD5 dan Konsep Penggunaannya

Dalam kriptografi, MD5 (*Message-Digest algortihm* 5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacammacam pada aplikasi keamanan, dan MD5 juga umum digunkan untuk melakukan pengujian integritas sebuah file. MD5 di desain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, MD4. Pada tahun 1996, sebuah kecacatan ditemukan dalam desainnya, walau bukan kelemahan fatal, pengguna kriptografi mulai menganjurkan menggunakan algoritma lain, seperti SHA-1 (klaim terbaru menyatakan bahwa SHA-1 juga cacat). Pada tahun 2004, kecacatan-kecacatan yang lebih serius ditemukan menyebabkan penggunaan algoritma tersebut dalam tujuan untuk keamanan jadi makin dipertanyakan.[5]

Konsep penggunaan md5 antara lain:

a. Kerahasiaan (*Confidentiality*). Sederhananya, kerahasiaan adalah proses penyembunyian data dari orang-orang yang tidak punya otoritas.
b. Integritas (*Integrity*) Proses untuk menjaga agar sebuah data tidak dirubah-rubah sewaktu ditransfer atau disimpan.
c. Penghindaran Penolakan (*Nonrepuditation*) Proses untuk menjaga bukti-bukti bahwa suatu data berasal dari seseorang. Seseorang yang ingin menyangkal bahwa data tersebut bukan berasal darinya, dapat saja melenyapkan bukti-bukti yang ada. Karenanya diperlukan teknik untuk melindungi data-data tersebut.
d. Autentikasi (*Authentication*) Proses untuk menjamin keaslian suatu data.
e. Tanda Tangan Data (*Data Signature*) Dapat disebut juga sebagai tanda tangan digital. Berguna untuk menandatangi data digital. Contohnya adalah *Digital Signature Algorithm* (DSA).
f. Kontrol Akses (*Access Control*) Untuk mengontrol akses terhadap suatu entity

3. Rancangan *Use Case Diagram*



Gambar 1. Diagram Proses User

Proses usecase diatas hanya memiliki 1 aktor yaitu user yang mempunyai task/tugas memasukkan data-datanya (*username dan password*) untuk dapat login kemudian user tersebut juga bisa mengganti password yang telah ia inputkan.

[4] Khairil and Prama Wira Ginta, "Implementasi Pengamanan Database Menggunakan MD5," *Jurnal Media Infotama* 8, no. 1 (2012): 29–44.
[5] Saipul Bahri et al., "Menggunakan METODE ENKRIPSI MD5 (Message-Digest Algorihm 5)," *Jurnal Ilmiah* 5, no. 5 (2012): 1–15.

Setelah user menginputkan username dan password, proses enkripsi akan dikerjakan dengan hanya mengenkripsi password user bersangkutan sedangkan username tetap dalam data yang tidak dienkripsi.

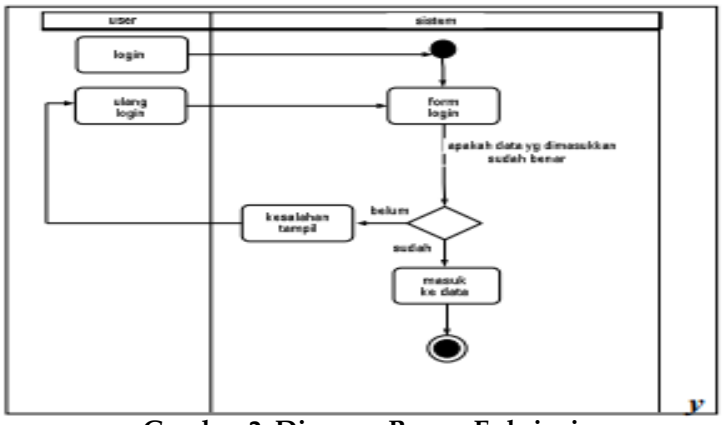
Dilihat dari gambar diatas bahwa pertama user memasukkan passwordnya kemudian akan di enkripsi oleh sistem, gambar berikutnya user melakukan login dengan password yang sama agar bisa masuk ke dalam sistem/menu utama. Sistem akan membaca/meng dekripsi apakah password yang dimasukkan sesuai dengan field password yang tersimpan jika sesuai sistem akan membaca apakah username yang dimasukkan juga sesuai, jika username dan password tersebut sesuai dengan pembacaan sistem, maka user bisa masuk atau login ke menu utama.[6]

Setelah berhasil masuk ke menu utama, pengguna akan disajikan dengan berbagai opsi menu dan fitur sesuai dengan hak akses yang telah ditetapkan. Setiap tindakan yang dilakukan oleh pengguna, seperti mengakses data tertentu, menambah atau mengedit informasi, serta melakukan transaksi lainnya, akan melalui proses verifikasi untuk memastikan bahwa hanya pengguna yang berwenang yang dapat melakukannya.

Untuk menjaga keamanan data, setiap transaksi dan perubahan yang dilakukan oleh pengguna akan dicatat dalam log aktivitas. Log ini mencakup informasi seperti waktu, tindakan yang dilakukan, dan identitas pengguna yang melakukannya. Hal ini penting untuk audit keamanan dan memastikan tidak ada akses atau perubahan yang tidak sah. Selain itu, sistem akan memantau aktivitas pengguna secara real-time. Jika terdeteksi adanya aktivitas yang mencurigakan, seperti percobaan login yang gagal berulang kali atau akses ke data sensitif dari lokasi yang tidak dikenal, sistem akan segera mengirimkan peringatan kepada administrator untuk tindakan lebih lanjut.

Untuk menambah lapisan keamanan, sistem juga dapat menggunakan mekanisme otentikasi multifaktor (MFA), di mana selain memasukkan password, pengguna juga harus melewati verifikasi tambahan seperti kode OTP (One-Time Password) yang dikirimkan ke perangkat mobile atau email terdaftar. Dengan demikian, meskipun password pengguna diketahui oleh pihak yang tidak berwenang, akses ke sistem tetap terlindungi. Seluruh mekanisme ini dirancang untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses dan melakukan perubahan di dalam sistem, serta untuk melindungi integritas dan kerahasiaan data dari ancaman keamanan.

4. *Activit Diagram*



Gambar 2. Diagram Proses Enkripsi

[6] Muhammad Wahyu Ade Saputra, Sri Ayu Ashari, and Esta Larosa, "Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data Dengan Enkripsi AES," *Inverted: Journal of Information Technology Education* 4, no. 2 (2024): 79–85.

Activity diagram diatas menggambarkan bagaimana alur dari user mulai dari user melakukan login sampai user memasuki menu utama dari sistem. Proses enkripsi diatas dapat dijelaskan sebagai berikut: user melakukan login melalui form login, jika data yang dimasukkan user sudah sesuai dengan data yang ada pada database maka proses akan turun kebawah dan selesai, jika data yang dimasukkan user tidak sesuai dengan data yang ada pada database maka user akan mengulangi proses menginput login melalui form login diatas.[7] Jika login berhasil, pengguna akan diarahkan ke menu utama di mana ia dapat mengakses berbagai fitur sesuai dengan hak aksesnya. Setiap tindakan yang dilakukan oleh pengguna, seperti mengakses data, menambah atau mengedit informasi, akan diverifikasi oleh sistem untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat melakukannya.

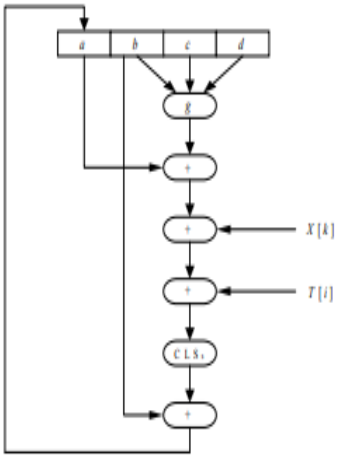
Proses verifikasi ini tidak hanya memastikan keaslian data yang dimasukkan, tetapi juga melibatkan enkripsi data yang diinputkan untuk menjaga kerahasiaan dan keamanan informasi. Setelah verifikasi berhasil, sistem akan mengizinkan akses ke fitur yang diminta.

Selain itu, untuk meningkatkan keamanan, sistem menggunakan berbagai metode enkripsi canggih yang terus diperbarui untuk mencegah akses yang tidak sah. Setiap kali pengguna mencoba untuk login atau mengakses data sensitif, sistem akan mengenkripsi data tersebut sebelum dikirimkan melalui jaringan.

Jika terdeteksi adanya aktivitas mencurigakan, seperti upaya login yang gagal berulang kali atau akses ke data dari lokasi yang tidak biasa, sistem akan mengaktifkan mekanisme perlindungan tambahan. Misalnya, sistem mungkin meminta verifikasi tambahan dari pengguna, seperti kode OTP (One-Time Password) yang dikirimkan ke perangkat mobile pengguna atau email terdaftar. Dengan seluruh mekanisme keamanan ini, sistem memastikan bahwa hanya pengguna yang sah yang dapat mengakses dan menggunakan fitur-fitur yang ada, serta melindungi integritas dan kerahasiaan data dari ancaman keamanan. Setiap langkah dalam proses ini dirancang untuk memberikan lapisan perlindungan tambahan yang diperlukan untuk menjaga keamanan sistem dan data pengguna.

5. Operasi Dasar MD5

Operasi dasar MD5 diperlihatkan pada Gambar berikut:



Gambar 3. Operasi Dasar MD5

Operasi dasar MD5 yang diperlihatkan pada Gambar di atas dapat ditulis dengan sebuah persamaan sebagai berikut:

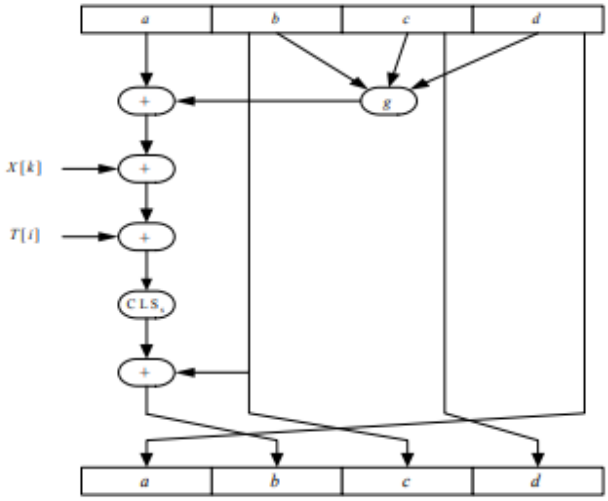
b + CLSs(a + g(b, c, d) + X[k] + T[i])←a

[7] Ibid.

keterangan:
a, b, c, d = empat buah peubah penyangga 32-bit A, B, C, D
g = salah satu fungsi F, G, H, I
CLSs = circular left shift sebanyak s bit
X[k] = kelompok 32-bit ke-k dari blok 512 bit message ke-q.
Nilai k = 0 sampai 15.
T[i] = elemen Tabel T ke-i (32 bit)
+ = operasi penjumlahan modulo 232

Karena ada 16 kali operasi dasar, maka setiap kali selesai satu operasi dasar, penyangga-penyangga itu digeser ke kanan secara sirkuler dengan cara pertukaran sebagai berikut: [8]

d←temp
c←d
b←c
a←b
temp←a



Gambar 4. Opesari Dasar MD5 (Message-Digest Algorihm 5)

Selain itu, implementasi sistem pencadangan basis data juga berdampak positif pada ketersediaan data. Pemulihan data yang cepat dan efisien dalam situasi darurat atau bencana membuktikan bahwa solusi keamanan yang diterapkan tidak hanya berfokus pada melindungi data dari serangan, tetapi juga menjamin kelangsungan operasional sistem secara keseluruhan.

Sistem pencadangan ini biasanya melibatkan proses backup rutin yang dilakukan secara otomatis dan disimpan di lokasi yang aman, baik lokal maupun cloud. Dengan demikian, data dapat dipulihkan dengan cepat jika terjadi kehilangan atau kerusakan sistem. Adanya cadangan data memungkinkan organisasi mengurangi waktu henti (downtime) dan memastikan layanan tetap tersedia bagi pengguna.

Pengujian berkala terhadap prosedur pemulihan juga merupakan bagian penting dari strategi ini. Pengujian ini memastikan bahwa dalam keadaan darurat, data dapat dipulihkan dengan benar dan operasional sistem dapat kembali normal secepat mungkin. Ini melibatkan simulasi berbagai skenario bencana dan mengevaluasi respons sistem terhadap masing-masing skenario.

[8] Ibid.

Selain itu, implementasi redundansi dalam infrastruktur IT memainkan peran penting dalam menjaga ketersediaan data dan layanan. Redundansi ini bisa berupa server cadangan, jalur komunikasi alternatif, dan mekanisme failover otomatis yang aktif ketika komponen utama gagal. Semua ini bekerja sama untuk memastikan bahwa gangguan pada satu bagian sistem tidak menyebabkan gangguan total pada layanan.

Dengan kombinasi strategi pencadangan, pengujian pemulihan, dan redundansi infrastruktur, organisasi dapat memastikan bahwa sistem mereka tidak hanya terlindungi dari ancaman, tetapi juga mampu bertahan dan pulih dari berbagai insiden yang dapat mengganggu operasional. Hal ini memberikan kepercayaan kepada pengguna bahwa data mereka aman dan layanan akan tetap berjalan lancar meskipun terjadi hal-hal yang tidak terduga.

6. Implementasi Pengamanan Database Dengan Oracle Security Server

Security server Adalah salah satu konsep dalam security jaringan dimana terdapat sever yang bertugas sebagai *authorization dan authentication* terhadap segala sesuatu tindakan yang akan masuk ke dalan sistem. Sementara Oracle Security Server Adalah suatu produk security dimana mendukung authorization tersentral dan *authentication* terdistribusi di dalam lingkungan Oracle. Authentication memberikan keyakinan bahwa yang mengakses satu atau lebih Oracle Database Server adalah valid. Authorization memberikan kepastian bahwa sekelompok orang yang telah diberi hak akses hanya dapat mengoperasikan menurut privelege dia dimana telah didefinisikan oleh seorang administrator.

Penerapan Teknologi Database Dalam Pengelolaan Data

Data bisnis yang efisien dan terorganisir dengan baik dapat memberikan keunggulan kompetitif bagi perusahaan, memungkinkan pengambilan keputusan yang tepat waktu dan strategis, serta memberikan wawasan yang berharga untuk pengembangan bisnis yang berkelanjutan.Salah satu teknologi yang secara luas diterapkan dalam pengelolaan data bisnis adalah teknologi database. Teknologi ini memungkinkan organisasi untuk menyimpan, mengelola, dan mengakses data dengan efisien dan aman. Dalam konteks ini, database merupakan entitas yang terpusat yang mengumpulkan dan menyimpan data yang relevan dengan kegiatan bisnis, termasuk informasi pelanggan, transaksi, inventaris, dan banyak lagi.

Penerapan teknologi database dalam pengelolaan data bisnis membawa sejumlah manfaat yang signifikan. Pertama, dengan menggunakan database, perusahaan dapat mengintegrasikan data dari berbagai sumber yang berbeda, termasuk sistem internal dan eksternal. Hal ini memungkinkan untuk menghasilkan gambaran yang komprehensif dan terpadu mengenai berbagai aspek bisnis.

Kedua, database juga memungkinkan penyimpanan data yang aman dan terstruktur.Dengan adanya mekanisme keamanan yang tepat,seperti izin akses yang terbatas dan enkripsi data, perusahaan dapat melindungi informasi penting mereka dari akses yang tidak sah atau kehilangan data yang tidak terduga. Selain itu, struktur yang terorganisir dari database memungkinkan pencarian dan analisis data yang efisien,mempercepat proses pengambilan keputusan.Selain itu,teknologi database juga memfasilitasi kemampuan untuk mengotomatiskan proses bisnis.Dengan menggunakan database,perusahaan dapat mengembangkan aplikasi perangkat lunak yang mengotomatiskan tugas- tugas rutin, seperti pengolahan pesanan, manajemen inventaris,atau pelacakan transaksi.

7. Memperkuat Keamanan Data melalui Teknologi Blockchain

Dalam konteks transformasi digital di Indonesia, penggunaan teknologi blockchain untuk keamanan data memiliki potensi yang besar untuk meningkatkan keamanan dan transparansi dalam pengelolaan data. Namun, penggunaan teknologi blockchain dalam transformasi digital di Indonesia masih tergolong baru dan

terbatas. [9]Sejumlah perusahaan dan institusi di Indonesia mulai mempertimbangkan penggunaan blockchain dalam bisnis mereka, tetapi masih banyak yang belum memahami potensi penuh dan kelemahan teknologi ini.

Selain itu, masalah teknis dan infrastruktur juga menjadi tantangan bagi pengembangan blockchain di Indonesia. Ketersediaan infrastruktur yang memadai, ketersediaan SDM yang memiliki keahlian dalam bidang blockchain, serta dukungan dari lembaga keuangan dan pemerintah menjadi faktor penting dalam pengembangan teknologi blockchain. Masalah-masalah teknis yang muncul dalam pengembangan blockchain di Indonesia termasuk skala jaringan yang terbatas, ketergantungan pada jaringan internet yang tidak selalu stabil, dan keterbatasan teknologi yang digunakan dalam transaksi blockchain. Meskipun demikian, teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan data dalam transformasi digital di Indonesia. Berbagai industri dan sektor yang terlibat dalam transformasi digital, seperti perbankan, logistik, dan pemerintahan, dapat memanfaatkan teknologi ini untuk meningkatkan keamanan data mereka.[10]

Peningkatan Transparansi Teknologi blockchain memiliki kemampuan untuk meningkatkan transparansi dalam pelaporan keuangan. Blockchain menciptakan catatan transaksi yang tidak dapat diubah dan dapat dilihat oleh semua pihak yang berwenang. Studi yang dilakukan oleh Dai dan Vasarhelyi menunjukkan bahwa blockchain dapat meningkatkan transparansi melalui pencatatan transaksi yang real-time dan auditable. Selain itu, blockchain juga memungkinkan akses terbuka dan transparan terhadap data keuangan, sehingga mengurangi risiko manipulasi data dan meningkatkan kepercayaan dari pemangku kepentingan.[11]

Dalam konteks kontrak di Indonesia, blockchain memberikan transparansi karena semua pihak yang terlibat dapat melihat kontrak, perubahan yang terjadi padanya, serta semua transaksi terkait. Ini dapat mengurangi potensi penipuan dan ketidaksetujuan dalam kontrak. Sistem blockchain adalah inovasi teknologi yang dapat digunakan untuk meningkatkan transparansi dan integritas data dalam transaksi kontrak di Indonesia. Dalam konteks ini, blockchain adalah ledger digital terdesentralisasi yang merekam dan memverifikasi transaksi menggunakan teknik kriptografi.[12]

8. Pemanfaatan Blockchain Akan Memiliki

Blockchain dapat menjamin seluruh transaksi node tanpa memerlukan pihak ketiga atau suatu supernode yang diberi otoritas lebih.[13] Penggunaan blockchain akan memastikan hubungan antar node dapat dipercaya, sehingga arsitektur menjadi optimal.

1. Penggunaan blockchain dapat menghindari terjadinya single point of failure . Hal ini dikarenakan jaringan blockchain merupakan jaringan terdistribusi, sehingga kegagalan pada beberapa node tidak akan menyebabkan kegagalan

[9] Ilham M. Said and Harunur Rasyid, "Implementasi Pengamanan Database Dengan Oracle Security Server," *Jurnal Fakultas Hukum UII* 2005, no. Snati (2005): 15

[10] Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia," *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68.

[11] Hengky Leon Ricky, Dedi Haryadi, "Pengaruh Implementasi Teknologi Blockchain Dalam Meningkatkan Transparansi Dan Keandalan Pelaporan Keuangan," *Journal Review Pendidikan dan Pengajaran* 7, no. 20 (2020): 8504818.

[12] Asep Hasanudin Leny Megawati, Cecep Wiharma, "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia," *Paper Knowledge . Toward a Media History of Documents* 9, no. 2 (2020): 12–26.

[13] Iswanto et al., "Pemanfaatan Teknologi Blockchain Di Bidang Pendidikan," *Tematik* 9, no. 2 (2022): 171–181.

2. Blockchain dapat memungkinkan pengguna untuk menyimpan dan menerima informasi tanpa takut adanya pemalsuan data.[14]

Selain untuk menyimpan informasi, teknologi Blockchain juga memungkinkan perpustakaan untuk mengaplikasikannya dalam hal publikasi ilmiah. Blockchain bisa digunakan untuk membuat versi dari artikel jurnal yang bisa dilakukan verifikasi dengan menggunakan cap waktu (time stamp). Selain itu teknologi Blockchain ini bisa juga digunakan dalam hal Manajemen Hak Digital perpustakaan. Hal ini sangat dimungkinkan karena Blockchain menciptakan catatan unik yang bisa diverifikasi serta bisa diakses oleh siapa saja. Salah satu contoh penerapan dari teknologi ini adalah NFT atau Non-Fungible Token yang akhir-akhir ini ramai menjadi perbincangan di kalangan pemerhati teknologi Blockchain. Sekalipun isu yang diperbincangan lebih berat dalam hal trading, lelang dan apresiasi nilai suatu karya seni digital, namun sebenarnya NFT memiliki kekuatan pada perlindungan hak cipta. NFT secara sederhana adalah token yang merepresentasikan kepemilikan atas suatu barang unik. NFT merupakan praktik asset tokenization yang bekerja di ekosistem blockchain. Dengan menjadikan suatu karya digital sebagai NFT, pada dasarnya kita memberikan perlindungan berupa sertifikat digital atas karya tersebut. [15]

Teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan database penduduk di Kemendagri. Implementasi blockchain dapat meningkatkan desentralisasi data, meningkatkan transparansi dan akuntabilitas, dan meningkatkan ketahanan terhadap serangan siber. Namun, terdapat beberapa tantangan yang perlu di addressed sebelum implementasi blockchain dapat dilakukan secara menyeluruh.[16] Diperlukan kerjasama antara pemerintah, akademisi, dan industri untuk mengatasi tantangan tersebut dan mewujudkan implementasi blockchain yang sukses untuk database penduduk di Indonesia.[17]

D. Kesimpulan

Penggunaan sistem informasi dan basis data telah menjadi hal yang sangat penting bagi berbagai institusi, termasuk pemerintah dan perusahaan, untuk mendukung operasional dan manajemen mereka. Database memiliki peran krusial dalam menyimpan dan mengelola informasi yang dibutuhkan untuk berbagai aplikasi, mulai dari e-Commerce hingga e-Business. Seiring dengan perkembangan teknologi, khususnya teknologi web, basis data kini sering diintegrasikan dengan aplikasi web untuk mengelola data pengguna secara efektif, seperti menyimpan nama pengguna, kata sandi, dan informasi kartu kredit. Keamanan dan kerahasiaan data menjadi isu penting, terutama dalam sistem penjualan, karena data yang disadap atau dibajak dapat menyebabkan kerugian besar. Oleh karena itu, dibutuhkan sistem yang mampu menangani keamanan database, salah satunya dengan menggunakan teknik enkripsi seperti MD5 dan teknologi blockchain. Meskipun telah ditemukan beberapa kelemahan pada enkripsi MD5, teknik ini tetap digunakan untuk memastikan kerahasiaan, integritas, dan autentikasi data.

E. Referensi-Referensi

Bahri, Saipul, Susan Dian Ps, Mahasiswa Universitas, Bina Darma, and Dosen Universitas. "Menggunakan Metode Enkripsi MD5 (Message-Digest Algorihm 5

[14] Ilham Alvendo Wahyu Aranski Farhan Hajid, Nur Saputra, Joseph Pasaribu, "Kriptosistem Berbasis Blockchain Untuk Berbagi Data Terpecaya Dalam Sistem Informasi Cloud," *Journal.Iteba.Ac.Id* 2, no. 2 (2023): 6–12

[15] Teguh Prasetyo Utomo, "Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan," *Buletin Perpustakaan* 4, no. 2 (2022): 173–200.

[16] Mesi Suharni Banurea and Muhammad Irwan Padli Nasution, "Penerapan Teknologi Database Dalam Data Bisnis," *Penerapan Teknologi Database Dalam Pengelolaan Data Bisnis* Vol.1, no. 3 (2023): 1–6.

[17] Chrisna Satya Wardhana, "Implementasi Teknologi Blockchain Dalam Optimalisasi Keamanan Database Penduduk Di Kementerian Dalam Negeri," *Action Research Literature* 8, no. 4 (2024): 642–648.

).” *Jurnal Ilmiah* 5, no. 5 (2012): 1–15.

Chrisna Satya Wardhana. “Implementasi Teknologi Blockchain Dalam Optimalisasi Keamanan Database Penduduk Di Kementerian Dalam Negeri.” *Action Research Literature* 8, no. 4 (2024): 642–648.

Farhan Hajid, Nur Saputra, Joseph Pasaribu, Ilham Alvendo Wahyu Aranski. “Kriptosistem Berbasis Blockchain Untuk Berbagi Data Terpecaya Dalam Sistem Informasi Cloud.” *Journal.Iteba.Ac.Id* 2, no. 2 (2023): 6–12. https://journal.iteba.ac.id/index.php/jurnalsiteba/article/view/137%0Ahttps://journal.iteba.ac.id/index.php/jurnalsiteba/article/download/137/148.

Gatot Susilo. “Keamanan Basis Data Pada Sistem Informasi Di Era Global.” *Jurnal TRANSFORMASI* 12, no. 2 (2016): 78–87.

Iswanto, Novianti Indah Putri, Zen Munawar, Rita Komalasari, and Dandun Widhiantoro. “Pemanfaatan Teknologi Blockchain Di Bidang Pendidikan.” *Tematik* 9, no. 2 (2022): 171–181.

Khairil, and Prama Wira Ginta. “Implementasi Pengamanan Database Menggunakan MD5.” *Jurnal Media Infotama* 8, no. 1 (2012): 29–44.

Leny Megawati, Cecep Wiharma, Asep Hasanudin. “PERAN TEKNOLOGI BLOCKCHAIN DALAM MENINGKATKAN KEAMANAN DAN KEPASTIAN HUKUM DALAM TRANSAKSI KONTRAK DI INDONESIA.” *Paper Knowledge . Toward a Media History of Documents* 9, no. 2 (2020): 12–26.

Ricky, Dedi Haryadi, Hengky Leon. “Pengaruh Implementasi Teknologi Blockchain Dalam Meningkatkan Transparansi Dan Keandalan Pelaporan Keuangan.” *Journal Review Pendidikan dan Pengajaran* 7, no. 20 (2020): 8504818.

Said, Ilham M., and Harunur Rasyid. “Implementasi Pengamanan Database Dengan Oracle Security Server.” *Jurnal Fakultas Hukum UII* 2005, no. Snati (2005): 15–19. https://www.neliti.com/id/publications/112099/implementasi-pengamanan-database-dengan-oracle-security-server.

Saputra, Muhammad Wahyu Ade, Sri Ayu Ashari, and Esta Larosa. “Keamanan Data Sistem Informasi Akademik ITEkes Mahardika: Penerapan Sistem Pencadangan Basis Data Dengan Enkripsi AES.” *Inverted: Journal of Information Technology Education* 4, no. 2 (2024): 79–85.

Subang, Stmik, and Enkripsi Kriptografi Gost. “Pengamanan Basis Data Sistem Penjualan Dengan Menggunakan Teknik Enkripsi Kriptograsi Gost.” *Jurnal Teknologi Informasi dan Komunikasi* 2, no. April (2018): 49–66.

Suharni Banurea, Mesi, and Muhammad Irwan Padli Nasution. “Penerapan Teknologi Database Dalam Data Bisnis.” *Penerapan Teknologi Database Dalam Pengelolaan Data Bisnis* Vol.1, no. 3 (2023): 1–6. https://doi.org/10.59024/jiti.v1i3.284.

Suryawijaya, Tito Wira Eka. “Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia.” *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68.

Utomo, Teguh Prasetyo. “Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan.” *Buletin Perpustakaan* 4, no. 2 (2022): 173–200.

Zalukhu, Kristovorus, Yohanni Syahra, and Trinanda Syahputra. “Implementasi Sistem Keamanan Database Data Pelanggaran Hukum Disiplin Prajurit Menggunakan Algoritma Advanced Encryption Standard 128 Bit Pada Pengadilan Militer I-02 Medan.” *J-SISKO TECH (Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD)* 3, no. 2 (2020): 138.