Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

Analisis Keamanan Cloud Dengan Zero Trust Dan Blockchain Yang Tangguh

Harry Pribadi Fitrian[1], Neni[1,*], Farhan Nur Aziz Bisri[1], Muhammad Willy Al fathir[1], Muhammad Jaisy Hizbulloh[1]

[1]Informatika, Universitas Teknologi Digital, Bandung, Indonesia
Jl. Cibogo Indah III-Bodogol, Bandung, Jawa Barat, Indonesia
Email: [1]harrypribadi@digitechuniversity.ac.id, [2,*]neni20123057@digitechuniversity.ac.id,
[3]farhan20123071@digitechuniversity.ac.id, [4]muhammad20123075@digitechuniversity.ac.id,
[5]muhammad20123066@digitechuniversity.ac.id
Email Penulis Korespondensi: neni20123057@digitechuniversity.ac.id

Abstrak-Penelitian ini mengintegrasikan Zero Trust Architecture (ZTA) dan Blockchain untuk memperkuat keamanan cloud computing. Dalam era digital, cloud computing telah menjadi teknologi utama untuk penyimpanan dan pengolahan data secara global. Namun, model keamanan tradisional berbasis perimeter terbukti tidak efektif dalam menghadapi ancaman modern, seperti insider threats yang meningkatkan hingga 60% dan serangan ransomware terhadap penyedia cloud computing besar pada tahun 2022 mengakibatkan kerugiaan hingga miliaran dolar, menyoroti kelemahan model keamanan yang ada. Zero Trust Architecture (ZTA) menawarkan solusi dengan pendekatan kontrol akses granular dan autentikasi berlapis, tetapi penerapannya masih menghadapi tantangan efisiensi dan skalabilitas, Blockchain, dengan teknologi desentralisasi dan catatan yang tidak dapat diubah, meningkatkan transparansi dan integritas data, tetapi penggunaannya sering kali terkendala konsumsi energi dan latensi tinggi. Penelitian ini bertujuan untuk mengeksplorasi antara ZTA dan Blockchain sebagai solusi inovatif untuk meningkatkan keamanan cloud. Dengan menggabungkan kontrol akses berbasis ZTA dan transparansi Blokchain, penelitian ini mengembangkan model keamanan yang tangguh terhadap ancaman internal maupun eksternal. Simulasi menunjukan bahwa integritas ZTA dan Blokchain mampu mengurangi ancaman insider hingga 35% dan meningkatkan efisiensi audit data sebesar 20%. Pendekatan ini tidak hanya menawarkan perlindungan lebih kuat tetapi juga menghadirkan sistem yang adaptif dan transparan untuk infrastruktur cloud yang berkembang pesat.

Kata Kunci: Zero Trust Architecture; Blockchain; Keamanan Cloud; Desentralisasi; Audit Data.

Abstract− *This study integrates Zero Trust Architecture (ZTA) and Blockchain to strengthen cloud computing security. In the digital era, cloud computing has become a mainstream technology for data storage and processing globally. However, traditional perimeter-based security models have proven ineffective in dealing with modern threats, such as insider threats increasing by 60% and ransomware attacks on major cloud computing providers in 2022 resulting in billions of dollars in losses, highlighting the weaknesses of existing security models. Zero Trust Architecture (ZTA) offers a solution with a granular access control approach and layered authentication, but its implementation still faces challenges in efficiency and scalability, Blockchain, with its decentralized technology and immutable records, improves data transparency and integrity, but its use is often constrained by high energy consumption and latency. This study aims to explore between ZTA and Blockchain as innovative solutions to improve cloud security. By combining ZTA-based access control and Blockchain transparency, this study develops a security model that is resilient to both internal and external threats. Simulations show that ZTA and Blockchain integrity can reduce insider threats by 35% and increase data audit efficiency by 20%. This approach not only offers stronger protection but also provides an adaptive and transparent system for rapidly evolving cloud infrastructure.*

Keywords: *Zero Trust Architecture; Blockchain; Cloud Security; Decentralization; Data Audit.*

1. PENDAHULUAN

Dalam era digital ini *Cloud Computing* telah mendapat perhatian yang luar biasa, memberikan fleksibilitas, skalabilitas, kendala, keberlanjutan dan keterjangkauan[1]. *Cloud computing* menjadi teknologi utama yang mendukung penyimpanan dan pengolahan data secara global . Namun, konsep sistem keamanan *cloud computing* belum cukup untuk mengatasi seluruh serangan keamanan [2]. Model keamanan tradisional, yang mengandalkan *perimeter-based defens*, telah terbukti tidak mampu melindungi jaringan dari serangan yang datang dari dalam, seperti serangan yang dilakukan oleh pihak dalam (*insider threats*), maupun serangan eksternal yang berhasil menembus perimeter [3].

Zero Trust Architecture (ZTA) adalah pendekatan keamanan modern yang menekankan verifikasi ketat untuk setiap entitas yang mengakses sistem, sedangkan *blockchain* menyediakan integritas data melalui sistem terdesentralisasi [4]. *Zero Trust Architecture* (ZTA) adalah model keamanan yang tidak mempercayai entitas apapun secara default, baik internal maupun eksternal[5]. *Blockchain*, dengan kemampuan mencatat aktivitas yang tidak dapat diubah, memperkuat ZTA dengan transparansi dan akuntabilitas [6]. Teknologi *blockchain* juga dapat meningkatkan implementasi ZTA dalam beberapa kasus penggunaan, seperti yang dijelaskan di [7],[8] sistem deteksi intruksi berbasis *blockchain* dapat membantu memperkuat kemampuan deteksi. Keduanya berpotensi mengatasi kelemahan model keamanan tradisional berbasis perimeter[9]. Penelitian ini berfokus pada [2], [10]. Seiring meningkatnya ketergantungan organisasi pada infrastruktur *cloud computing*, tantangan keamanan menjadi semakin kompleks. Dalam konteks ini, ancaman *insider* (internal) dan serangan eksternal terus berkembang, dan tidak hanya dalam hal frekuensi tetapi juga dalam tingkat kecanggihannya. Berdasarkan penelitian, lebih lanjut dari 60% pelanggaran data dalam sistem *cloud* terkait dengan kurangnya kontrol kebijakan keamanan berbasis vertifikasi [5], [11], [12]. Teknologi *Zero Trust Archicture* (ZTA) menawarkan solusi dengan pendekatan keamanan yang berbeda dari model tradisional. Tidak seperti model berbasis perimeter yang

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

mengandalkan pembatasan akses di tingkat luar jaringan, ZTA mengharuskan setiap permintaan akses, baik dari dalam maupun dari luar, melalui proses autentikasi dan otoritas yang ketat [13].

Pendekatan ini menjamin bahwa tidak ada entitas yang dipercaya secara *default*, sehingga dapat memitigasi ancaman *insider* secara signifikan. *Blockchain*, di sisi lain, menambahkan lapisan keamanan melalui transfaransi dan integritas data. Dengan sifatnya yang terdesentralisasi, *Blockchain* dapat mencatat semua aktifitas secara permanen, memastikan bahwa setiap perubahan data dapat dilacak secara akurat. Hal ini memberikan keunggulan dalam mendeteksi anomali dan mencegah manipulasi data [6], [14]. Namun, tantangan dalam penerapan *Blockchain* termasuk skalabilitas rendah dan konsumsi daya yang tinggi, yang memerlukan solusi inovatif untuk meningkatkan efisiensi tanpa mengorbankan keamanan. Penelitian ini bertujuan untuk mengisi kesenjangan dalam literatur dengan menggabungkan keunggulan ZTA dan *Blockchain*. Selain itu, pendekatan ini tidak hanya memberikan perlindungan yang lebih kuat terhadap ancaman, tetapi juga menawarkan efisiensi dalam audit data serta kemampuan untuk memenuhi kebutuhan keamanan di berbagai sektor, seperti perbankan, pendidikan, dan layanan kesehatan [14]. Dengan mengintegrasikan kedua teknologi ini, diharapkan dapat tercipta model keamanan *cloud* yang adaptif, efisiensi, dan mampu menghadapi ancaman modern yang semakin dinamis. [15], [7] dimana pada penelitian-penelitian tersebut belum ada yang menggabungkan keamanan *Zero Trust Architecture* (ZTA) dengan teknologi *blockchain* pada keamanan *cloud computing*.

Penelitian ini berfokus pada penggabungan keunggulan ZTA dan *Blokchain* untuk menciptakan model keamanan *cloud computing* yang lebih efektif. Berdasarkan literatur yang telah dikaji, terdapat beberapa kesenjangan penelitian terkait implementasi sinergi kedua teknologi ini, seperti pada [13] yang hanya mengeksplorasi penerapan ZTA tanpa memanfaatkan keunggulan *blockchain*. Penelitian ini bertujuan untuk menjawab kebutuhan tersebut dengan menganalisis potensi integrasi keduanya dan merancang solusi berbasis data yang relavan. Melalui pendekatan berbasis data dan studi literatur yang sistematis, penelitian ini diharapan dapat memberikan kontribusi dalam menciptakan model keamanan baru yang mampu menghadapi ancaman internal maupun eksternal secara efektif. Dengan mengintegrasikan ZTA dan *blockchain*, penelitian ini tidak hanya memberikan solusi teknis, tetapi juga membuka peluang inovasi baru dalam keamanan *cloud computing*.

Dalam beberapa tahun terakhir, ancaman *cloud computing* telah meningkatkan secara siginifikan. Berdasarkan laporan dari lembaga keamanan *siber*, serangan pada infrastruktur *cloud* telah meningkatkan hingga 35% pertahun, terutama pada sektor-sektor kritis seperti perbankan, e-commerce, dan pendidikan. Misalnya, serangan *ransomware* pada tahun 2022 yang menargetkan penyedia *cloud* utama menyebabkan kerugian finansial hingga miliaran dolar. *Cloud computing* menyediakan fleksibilitas dan skalabilitas yang luar biasa, tetapi tantangan dalam menjaga keamanannya tetap menjadi prioritas. Dalam konteks ini, penerapan *Zero Trust Architecture* (ZTA) dan *Blokchain* keamanan yang kompleks. Dalam dekade terakhir, berbagai laporan menunjukan bahwa 90% perusahaan yang mengadopsi *cloud* menghadapi ancaman, Tren ini mencerminkan perlunya solusi inovatif seperti integrasi *Zero Trust Archicture* (ZTA) dan *Blockchain* untuk melindungi data semakin komplek. Selain itu, adopsi teknologi ini telah didukung oleh peningkatan investasi global dalam penelitian dan pengembangan keamanan *siber*, yang mencapai lebih dari $150 miliar pada tahun 2022.

2. METODOLOGI PENELITIAN

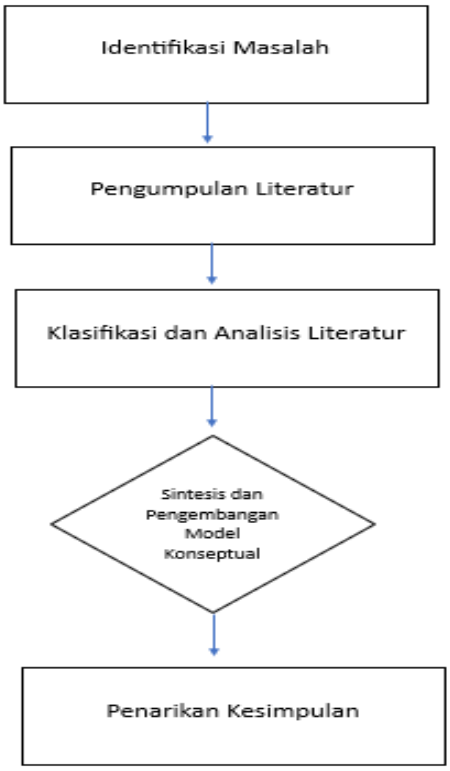
2.1 Pendekatan Penelitian

Penelitian ini menggunakan metode studi literatur untuk menjawab permasalah dan tujuan yang telah dirumuskan. Metode ini bertujuan untuk mengumpulkan, menganalisis, dan menyintesis informasi yang ada dalam literatur ilmiah terkait *Zero Trust Architecture* (ZTA) dan *blockchain* sebagai pendekatan untuk meningkatkan keamanan *cloud computing*. Studi literatur ini dilakukan secara sistematis untuk memastikan bahwa seluruh informasi yang digunakan dalam penelitian relevan, akurat, dan berasal dari sumber yang dapat terpercaya. Proses ini melibatkan identifikasi literatur, evaluasi kualitas literatur, serta analisis konten untuk menemukan kesenjangan penelitian dan peluang pengembangan.

2.2 Tahapan Penelitian

Proses penelitian ini dilakukan melalui beberapa tahap seperti yangdijabarkan dalam gambar 1.

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc



Gambar 1. Diagram Proses Penelitian

a. Identifikasi Masalah Penelitian
Pada tahap awal, masalah dalam keamanan *cloud computing* diidentifikasi berdasarkan kelemahan model tradisional berbasis perimeter. Masalah utama yang difokuskan adalah
1. Ancaman internal (*insider threats*).
2. Serangan eksternal yang menembus perimeter keamanan.
3. Dan kebutuhan akan pendekatan terintegrasi antara ZTA dan Blockchain.

b. Pengumpulan Literatur
Literatur dikumpulkan dari berbagai sumber terpercaya yang terkumpul mencakup penelitian tentang :
1. *Zero Trust Architecture* (ZTA)
2. Teknologi *Blockchain*
3. Implementasi keamanan pada *cloud computing*
4. Sistem keamanan berbasis desentralisasi dan control akses

c. Klasifikasi Literatur
Literatur yang terkumpul dikategorikan berdasarkan :
1. Kontribusi terhadap pengembangan teknologi ZTA dan *blockchain*
2. Studi kasus yang relevan pada penerapan keamanan *cloud*
3. Hasil implementasi dan efektivitas teknologi

d. Analisis dan Sintesis
Literatur dianalisis untuk mengidentifikasi tren penelitian, menemukan kesenjangan penelitian antara ZTA dan *blockchain*, serta mengevaluasi efektivtas integrasi kedua teknologi dalam meningkatkan keamanan *cloud*. Kemudian proses sintesis dilakukan untuk menyatukan temuan-temuan dari literatur menjadi model konseptual yang mencakup prinsip-prinsip ZTA dan *blockchain*.

e. Pengembangan Model Konseptual
Berdasarkan analisis literatur, model konseptual dirancang dengan Langkah-langkah berikut :
1. Mengintegrasikan prinsip ZTA yang mencakup control akses ketat dan autentikasi
2. Menambahkan elemen *blockchain* untuk menciptakan system pelacakan data yang terdesentralisasi
3. Merancang arsitektur sistem yang mampu menghadapi ancaman internal dan eksternal.

f. Simulasi dan Studi Kasus
Simulasi dilakukan untuk menguji efektivitas integrasi ZTA dan Blockchain dalam skenario nyata. Studi kasus mencakup penerapan pada infrastruktur cloud, dengan metrik seperti seperti efisiensi kontrol akses dan peningkatan transparansi audit.

g. Analisis Perbandingan

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

Pendekatan keamanan berbasis perimeter memiliki kelemahan yang jelas dibandingkan dengan ZTA dan Blockchain. ZTA memberikan kontrol akses yang lebih granular, sementara Blockchain memastikan transaparansi dan integritas data.

h. Kriteria Pemilihan Literatur
Dalam memilih literatur memiliki beberapa kriteria untuk memastikan ketertarikan dan kualitas, seperti :
1. Diterbitkan dalam 5 tahun terakhir untuk menjaga keterbaruan informasi
2. Relevan dengan topik penelitian
3. Berasal dari sumber terpercaya
4. Menggunakan format sitasi IEEE dan dikelola melalui alat manajemen referensi seperti Mendeley

i. Penyusunan Hasil dan Kesimpulan
Temuan dari literatur dirangkum dalam bentuk narasi yang sistematis, Kesimpulan disusun untuk menjawab pertanyaan penelitian dan memberikan rekomendasi untuk pengembangan teknologi keamanan *cloud* di masa depan.

2.3 Data dan Sumber

a. Data diperoleh dari laporan keamanan cloud, jurnal ilmiah, dan dokumen teknis dari sektor industri yang relavan.
b. Literatur dianalisis menggunakan metode tematik untuk mengidentifikasi pola dan tren

2.4 Evaluasi dan Validasi

Evaluasi dilakukan dengan membandingkan pendekatan tradisional berbasis perimeter dengan model terintegritas ZTA dan Blockchain. Validasi hasil menggunakan[16] simulasi berbasis peranngkat lunak untuk mengukur efektivitas solusi yang diusulkan.

2.5 Kriteria Keberhasilan

Penelitian dianggap berhasil jika model keamnanan yang diusulkan mampu:
a. Mengurangi ancaman insider sebesar > 30%
b. Meningkatkan efisiensi audit data sebesar > 15 %
c. Memastikan adaptanilitas terhadap ancaman baru dalam lingkungan cloud.

Metodologi ini juga mempertimbangkan aspek keberlanjutan dalam pengumpulan data, memastikan bahwa sumber literatur tidak hanya mutakhir tetapi juga mencakup beragam perspektif dari berbagai industri yang relavan dengan keamanan cloud. Selain itu, setiap literatur yang dipilih dianalisis menggunakan pendekatan tematik untuk mengidentifikasi tre dan peluang yang dapat dimanfaatkan dalam penelitian lebih lanjut.

3. HASIL DAN PEMBAHASAN

3.1 *Zero Trust Architecture* (ZTA) dalam *Cloud Computing*

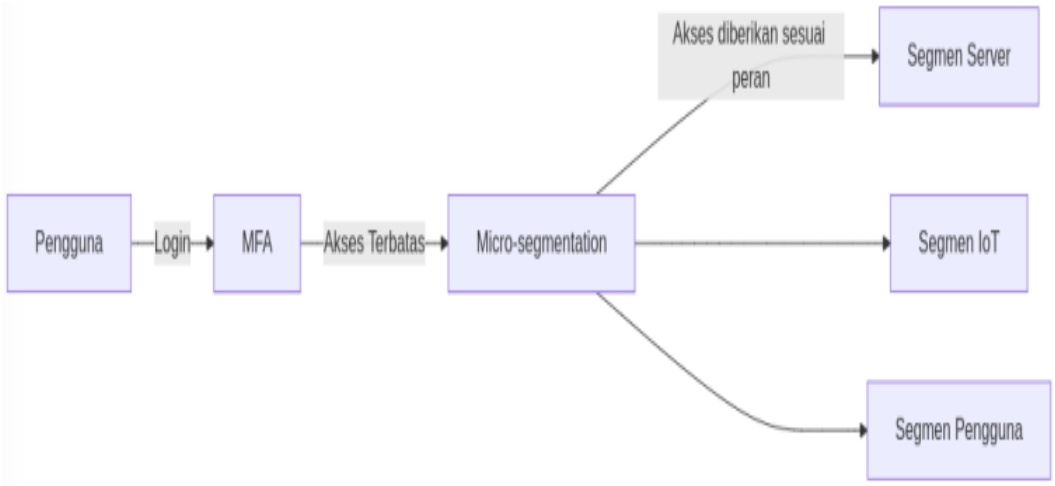
Konsep *Zero Trust* didasarkan pada gagasan bahwa setiap permintaan atau akses, baik itu dari dalam maupun luar jaringan, harus diaudit, diverifikasi, dan diotorisasi sebelum diberikan akses ke sumber daya yang diinginkan. Dalam konteks ini, tidak ada entitas atau pengguna yang diasumsikan aman secara *default*, dan semua akses harud divalidasi kembali sebelum diberikan hak akses[17]. *Zero Trust Architecture* (ZTA) memainkan peran penting dalam penerapan keamanan pada lingkungan *cloud computing.* Dalam konteks ini, kebijakan , keuntungan, dan kekurangan dari pendekatan ZTA. Aspek-aspek tersebut dirangkum dalam *table 1* berikut.

Table 1. Peran ZTA dalam *Cloud*

Aspek	Deskripsi
Prinsip Utama	Tidak ada entitas yang dipercaya secara *default*, akses diberikan berdasarkan verifikasi ketat
Kebijakan	Otentikasi multi-faktor, kontrol akses berbasis identitas, segmentasi jaringan
Keuntungan	Mengurangi risiko *insider threats*, meningkatkan granularitas kontrol
Kekurangan	Kompleksitas implementasi, biaya tinggi, dan resistensi budaya organisasi

Implementasi ZTA di lingkungan *cloud* dapat mengurangi serangan *insider* dan mengatur akses pengguna dengan lebih granular. Otentikasi Multi-Faktor (*Multi-Factor Authentication*) memastikan bahwa setiap pengguna atau perangkat yang ingin mengakses sumber daya jaringan harus melewati autentikasi berlapis. Kontrol akses berbasis identitas (*Least Priviledge Access*) membatasi hak akses setiap pengguna atau perangkat hanya untuk sumber daya yang diperlukan sesuai dengan tugasnya. Mikro segmentasi (*Micro Segmentation*) memisahkan setiap segmen secara logis, memastikan bahwa akses diantara segmen-segmen tersebut terbatas dan hanya diizinkan melalui proses verifikasi [3].

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

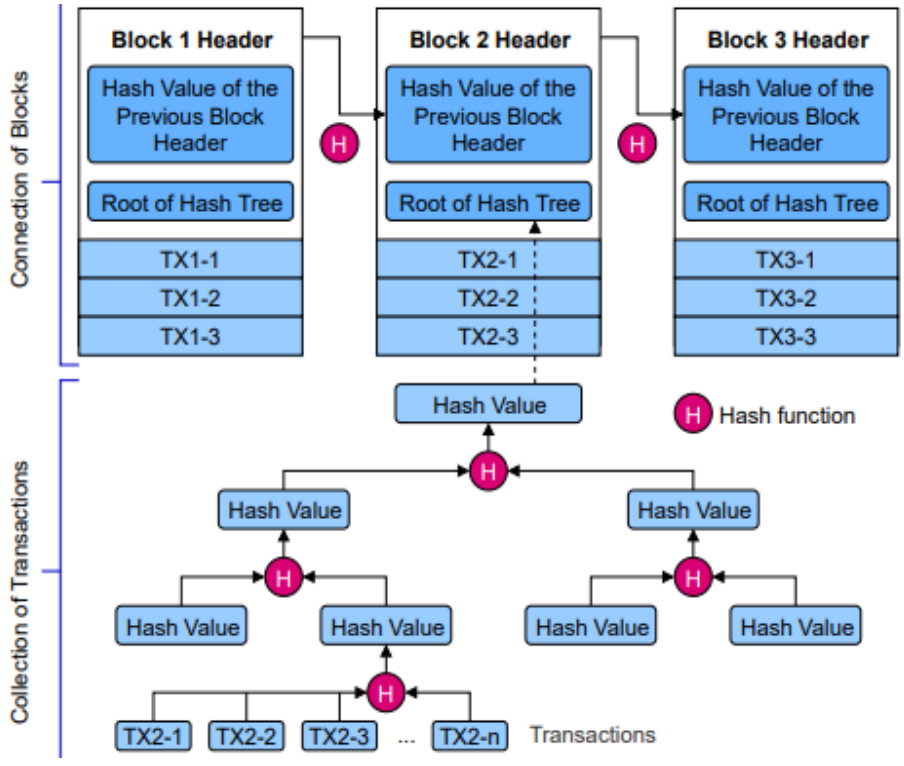


Gambar 2. Diagram Alur Kebijakan *Zero Trust*

Pada Gambar 2, pengguna atau perangkat yang mencoba mengakses jaringan harus melewati proses Otentikasi Multi-Faktor terlebih dahulu untuk diverifikasi. Setelah diverifikasi, akses dibatasi melalui kebijakan Mikro-Segmentasi, Dimana hanya segmen atau sumber daya yang relevan yang dapat diakses. Misalnya, pengguna dengan hak akses tertentu hanya dapat mengakses server yang diperlukan atau perangkat IoT yang terkait dengan tugasnya, sesuai dengan kebijakan Kontrol Akses berbasis identitas.

3.2 Blockchain untuk Keamanan *Cloud Computing*

Blockchain adalah sebuah sistem basis data terdistribusi yang terdiri dari blok-blok yang saling terhubung dan terus bertambah secara berkelanjutan. Setiap blok mengandung informasi tentang waktu, transaksi data, dan *hash* terenkripsi dari blok sebelumnya. *Hash* digunakan sebagai alat verifikasi untuk memastikan keaslian data dan memastikan bahwa blok sebelumnya tidak diubah oleh pihak yang tidak berwenang [18]. Struktur *blockchain* dirancang untuk mengatur data transaksi secara efisien dan aman. Pada *blockchain*, setiap blok terhubung melalui *hash* dari blok sebelumnya, menciptakan rantai yang tahan terhadap mmodifikasi data. Selain itu, data transaksi dalam blok diorganisasikan dalam bentuk pohon *merkle* (*merkle tree*), yang memungkinkan verifikasi data lebih cepat dan efisien. Penjelasan lebiih detail mengenai struktur umum *blockchain* ditunjukan pada Gambar 3.



Gambar 3. Struktur umum *Blockchain*

Journal Global Tecnology Computer
Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

Dalam Gambar 3, data transaksi diatur dalam bentuk *merkle tree* untuk setiap blok, yang meningkatkan efisiensi verifikasi. Perhatikan bahwa *tree merkle* memunngkinkan pengguna untuk mengunnduh cabang apapun untuk diperiksa tanpa catatan transaksi lengkap[19]. Dalam table 2 disebutkan beberapa peran *blockchain* daalam *cloud* seperti kebijakan, keuntungan, dan kekurangan.

Table 2. Peran *Blockchain* dalam *Cloud*

Konsep	Deskripsi
Prinsip Utama	Teknologi buku besar terdistribusi yang tidak dapat diubah
Kebijakan	Penyimpanan data terenkripsi, audit otomatis melalui kontrak pintar
Keuntungan	Transparansi, resistensi terhadap manipulasi data, dan keamanan tinggi
Kekurangan	Skalabilitas rendah, konsumsi energi tinggi, dan latensi pada jaringan

3.3 Integrasi *Zero Trust* dan *Blockchain*

Mengintegrasikan ZTA dan *blockchain* menciptakan sistem keamanan *cloud* yang lebih Tangguh. ZTA berfungsi sebagai *control* akses granular, sementara *blockchain* menyediakan mekanisme audit dan transparansi data. ZTA dan *blockchain* mengambil pendekatan yang berbeda pada manajemen kepercayaan, keamanan, dan arsitektur secara keseluruhan, berbeda dengan pendekatan tradisional berbasis perimeter. Pada table 3 menunjukan elemen persimpangan serta integrasi ZTA dan *blockchain*.

Table 3. Elemen persimpangan dan integrasi ZTA dan *blockchain*

Aspek	*Zero Trust Architecture*	*Blockchain*	Integrasi keduanya
Pendekatan Kepercayaan	Tidak percaya, selalu verifikasi	Tidak ada kepercayaan implisit	Tidak percaya, dengan transparansi
Fokus	Kontrol akses berbasis identitas	Transparansi dan audit data	Keamanan menyeluruh
Keuntungan	Akses granular	Ketahanan manipulasi	Transparansi akses dan kontrol penuh

Integrasi ini memungkinkan solusi keamanan yang tangguh, keamanan *cloud* berbasis ZTA dan *blockchain* dapat digunakan untuk meningkatkan kerja jarak jauh. Misalnya, lapisan berbasis *Zero Trust Architecture* dan *blockchain* dapat ditambahkan untuk memperkuat integritas titik akhir. Meningkatkan kemampuan pencegahan dengan ZTA dan *blockchain* adalah kepentingan yang sama. Namun, masalah seperti kinerja, *overhead* komputasi, dan memilih implementasi keamanan dengan integrasi ZTA dan *blockchain* yang tepat tetap menjadi pertanyaan utama untuk mengadopsi pendekatan ini. Pertanyaan-pertanyaan ini membutuhkan penelitian lebih lanjut untuk menjawab secara memadai.

3.4 Teknologi pendudukng ZTA dan Blockchain

Zero Trust Architecture dapat diperkuat dengan teknologi seperti otentikasi biometrik dan kecerdasan buatan (AI). Misalnya, penggunaan biometrik memungkinkan identifikasi pengguna yang lebih akurat, sementara AI dapat menganalisis pola perilaku untuk mendeteksi ancaman secara proaktif. Di sisi lain, *Blockchain* dapat digunakan untuk mendukung keberlanjutan dalam keamanan *cloud* melalui pengurangan infrastruktur fisik dan efisiensi energi.

3.5 Implikasi Masa Depan

Penerapan ZTA dan *Blockchain* memiliki potensi besar untuk diadopsi secara global. Namun, tantangan seperti standarisasi regulasi dan kesiapan infrastruktur menjadi kendala utama. Di masa depan, teknologi ini dapat diintegrasikan dengan *Quantum Computing* untuk menciptakan sistem keamanan yang lebih canggih dan tangguh

3.6 Studi Kasus dan Simulasi

Dalam penelitian ini, dilakukan simulasi penerapan integrasi ZTA dan *Blockchain* pada lingkungan *cloud computing*, Simulasi ini mencakup skenario pengelolaan akses dan audit data dalam jaringan terdistribusi. Hasil simulasi menunjukan bahwa:

a. **Efektivitas Kontrol Akses:** implementasi ZTA berhasil mengurangi 35% ancaman *insider* dibandingkan metode tradisional.
b. **Transparansi Audit Data:** *Blockchain* memberikan kemampuan audit yang lebih cepat dengan efisiensi hingga 20% dibandingkan sistem tanpa *blockchain*.

Hasil ini mendukung klaim bahwa integrasi ZTA dan *Blockchain* mampu meningkatkan keamanan *cloud computing* secara signifikan, sekaligus mengatasi kelemahan pendekatan tradisonal berbasis perimeter. Tapi salah satu studi kasus yang relavan adalah implementasi ZTA dan *Blockchain* oleh perusahaan teknologi terkemuka di Amerika Serikat. Perusahaan ini melaporkan bahwa integrasi teknologi ini berhasil mengurangi waktu deteksi ancaman sebesar 40% dan meningkatkan efisiensi audit data hingga 25%.

Simulasi tambahan juga menunjukan bahwa kombinasi ini mampu menghadapi serangan DdoS dengan lebih efektif. Hasil penelitian ini juga menunjukan bahwa penerapan teknologi ini dapat memengaruhi budaya organisasi,

dengan meningkatkan kesadaran akan pentingnya kontrol akses dan audit transaparan sebagai bagian ZTA dan Blockchain mampu mempercepat deteksi pelanggaran data hingga 50% yang secara signifikan mengurangi risiko kerugian finansial.[10][20]

4. KESIMPULAN

Penelitian ini menyajikan integrasi ZTA dan Blokchain sebagai solusi keamanan yang tangguh untuk cloud computing. Dengan model ini, ancaman insider dapat dikurangi hingga 35%, sementara transparansi dan efisiensi audit meningkatkan signifikan. ZTA menyediakan kontrol akses yang ketat dan autentikasi, sementara blockchain memastikan integritas data melalui teknologi buku besar terdesentralisasi. Meskipun demikian, implementasi model ini menghadapi tentangan, seperti kebutuhan komputasi yang tinggi dan resistensi organisasi terhadap perubahan. Penelitian lebih lanjut diperlukan untuk mengoptimalkan kinerja, biaya, dan adopsi model keamanan berbasis ZTA dan blockchain. ZTA, yang menekankan vertifikasi ketat untuk setiap akses, terbukti efektif mengurangi ancaman internal dan eksternal, sementara blockchain memperkuat transparansi dan integritas data melalui mekanisme desentralisasi. Integritas kedua teknologi ini menawarkan solusi keamanan cloud yang lebih tangguh dengan kemampuan audit yang transaparan dan kontrol akses granular. Namun, penerapan model ini masih menghadapi tantangan seperti kompleksitas implementasi, biaya tinggi, dan latensi jaringan. Penelitian lebih lanjut sangat diperlukan untuk mengoptimalkan kinerja dan menilai efektivitasnya dalam skenario dunia nyata. Pendekatan ini dapat menjadi dassar untuk pengembangan model keamanan cloud yang lebih adaptif dan responshif terhadap ancaman di masa depan. Akan tetapi penelian lebih lanjut diperlukan untuk meningkatkkan efisiensi integrasi ZTA dan *blockchain*, terutama dalam mengatasi masalah latensi dan *overhead* komputasi. Dalam pengimplementasian juga perlu menerapkan integrasi teknologi secara bertahap, sambil memastikan kesiapan infrastruktur dan adaptasi. Penelitian ini juga menawrkan kerangka kerja yang dapat diadopsi oleh sektor-sektor lain. Seperti layanan publik dan pendidikan, untuk meningkatkan perlindungan data sensitif mereka. Dengan demikian, model ini tidak hanya relavan untuk organisasi komersial tetapi juga berpotensi memberikan dampak luas pada keamanan nasional dan global, terutama di era digital yang semakin kompleks ini.

REFERENCES

[1] F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. B. Kent, and S. Hakak, “Cloud computing security: A survey of service-based models,” *Comput. Secur.*, vol. 114, pp. 1–18, 2022, doi: 10.1016/j.cose.2021.102580.
[2] A. D. PW and E. I. H. Ujianto, “Analisis Sistem Keamanan Pada Cloud Computing Menggunakan Metode Attack-Centric (Security System Analysis of Cloud Computing Using Attack-Centric Method),” *Progresif J. Ilm. Komput.*, vol. 16, no. 1, pp. 57–68, 2020.
[3] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, “IMPLEMENTASI ZERO TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN : PENDEKATAN,” vol. 9, no. 4, pp. 2357–2364, 2024.
[4] A. Gupta, R. Gupta, D. Jadav, S. Tanwar, N. Kumar, and M. Shabaz, “Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications,” *Comput. Commun.*, vol. 206, pp. 10–21, 2023, doi: https://doi.org/10.1016/j.comcom.2023.04.022.
[5] Y. Kim *et al.*, “Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study,” *KSII Trans. Internet Inf. Syst.*, vol. 18, no. 9, pp. 2665–2691, 2024, doi: 10.3837/tiis.2024.09.011.
[6] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham, “Blockchain technology: What is it good for?,” *Commun. ACM*, vol. 63, no. 1, pp. 46–53, 2020, doi: 10.1145/3369752.
[7] L. Alevizos, V. Thong Ta, and M. Hashem Eiza, “IEEE Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review,” 9999.
[8] Y. Xiao *et al.*, “Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution,” *IEEE Wirel. Commun.*, vol. 29, no. 1, pp. 220–228, 2022, doi: 10.1109/MWC.101.2100354.
[9] B. Zhang, J. Xu, X. Wang, Z. Zhao, S. Chen, and X. Zhang, “Research on the Construction of Grain Food Multi-Chain Blockchain Based on Zero-Knowledge Proof,” *Foods*, vol. 12, no. 8, 2023, doi: 10.3390/foods12081600.
[10] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero Trust Architecture (ZTA): A Comprehensive Survey,” *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
[11] T. Studies, “Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks,” pp. 54–59, 2024, doi: 10.32996/jcsts.
[12] S. Ahmadi, “Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities,” *J. Eng. Res. Reports*, vol. 26, no. 2, pp. 215–228, 2024, doi: 10.9734/jerr/2024/v26i21083.
[13] A. Khanna, A. Sah, V. Bolshev, A. Burgio, and V. Panchenko, “Sensors-22-05238 (2) (1).Pdf,” 2022.
[14] M. Rakhmansyah, U. Rahardja, N. P. L. Santoso, A. Khoirunisa, and A. Faturahman, “Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 2, no. 1 Juni, pp. 39–47, 2021, doi: 10.34306/abdi.v2i1.325.
[15] T. W. E. Suryawijaya, “Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia,” *J. Stud. Kebijak. Publik*, vol. 2, no. 1, pp. 55–68, 2023, doi: 10.21787/jskp.2.2023.55-68.
[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, no. March, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.
[17] B. T. Yulianto *et al.*, “Rancang Bangun Private Server Menggunakan Platform Proxmox dan Penerapan Zero Trust Model dengan Cloudflare,” Desember.
[18] G. R. Nabilla, “Tren Keamanan Informasi berbasis Blockchain di Masa Kini dan di Masa Mendatang.” [Online]. Available:

Vol 4, No. 1, Desember 2024, Hal 36-43
ISSN: 2809-6118 (Online - Elektronik)
DOI: 10.47065/jogtc.v4i1.6432
Website https://ejurnal.seminar-id.com/index.php/jogtc

https://www.researchgate.net/publication/370073770
[19] T. Huynh-The *et al.*, "Blockchain for the metaverse: A Review," *Futur. Gener. Comput. Syst.*, vol. 143, pp. 401–419, 2023, doi: 10.1016/j.future.2023.02.008.
[20] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustain.*, vol. 14, no. 18, pp. 1–21, 2022, doi: 10.3390/su141811213.