BIOS : Jurnal Teknologi Informasi dan Rekayasa Komputer
Vol. 7, No. 2, September 2026, hlm. 173 - 183
e-ISSN: 2722-0850

Arsitektur *API Gateway* pada *Hybrid Cloud* Berbasis *Zero Trust* untuk Perbankan Digital

B. Junedi Hutagaol[1], Riama Santy Sitorus[2], Nadya Allia Putri[3]
[1]Information System, Asa University, junedi@asaindo.ac.id
[2]Information Technology, Asa University, riama@asaindo.ac.id
[3]Information System, Asa University, nadiaap@gmail.com

Keywords:

Hybrid Cloud Architecture,
Zero Trust Security,
Digital Banking,
API Gateway,
Cyber Security

ABSTRACT

The expansion of digital banking ecosystems has accelerated the utilization of Application Programming Interfaces (APIs) to support service integration, transaction processing, and connectivity with external platforms. This increasing dependency on API-based services also creates new security challenges, requiring financial institutions to achieve a balance between protection, scalability, and regulatory obligations. This research proposes a Hybrid Cloud API Gateway Architecture incorporating Zero Trust Security principles to strengthen digital banking security. The study adopts the Design Science Research (DSR) methodology through several activities, including problem identification, requirement analysis, architecture development, expert assessment, and evaluation. The proposed architecture integrates API Gateway capabilities, Hybrid Cloud deployment strategies, and Zero Trust security controls to support secure, scalable, and resilient banking services. Sensitive workloads are maintained within controlled environments, while scalable services utilize public cloud capabilities to improve operational flexibility and resource efficiency. The evaluation results demonstrate that the proposed architecture is aligned with NIST SP 800-207 Zero Trust principles, addresses key risks from the OWASP API Security Top 10, and supports compliance considerations related to PCI DSS and ISO/IEC 27001. This research provides an architectural model that can support financial institutions in developing secure and adaptable digital banking platforms.

Kata Kunci:

Arsitektur *Hybrid Cloud*,
Zero Trust Security,
Digital Banking,
API Gateway,
Keamanan Siber

ABSTRAK

Transformasi layanan perbankan digital telah meningkatkan pemanfaatan *Application Programming Interface* (API) sebagai sarana integrasi layanan, pemrosesan transaksi, dan konektivitas dengan pihak eksternal. Kondisi ini memperluas kebutuhan terhadap mekanisme keamanan yang mampu mendukung skalabilitas layanan sekaligus memenuhi tuntutan regulasi. Penelitian ini mengusulkan *Hybrid Cloud API Gateway Architecture* dengan penerapan prinsip *Zero Trust Security* untuk memperkuat keamanan siber pada sistem perbankan digital. Pendekatan penelitian menggunakan *Design Science Research* (DSR) yang mencakup identifikasi masalah, analisis kebutuhan, perancangan arsitektur, validasi ahli, dan evaluasi. Arsitektur yang dihasilkan menggabungkan kapabilitas API *Gateway*, strategi *Hybrid Cloud Architecture*, dan kontrol keamanan berbasis *Zero Trust* untuk mendukung layanan perbankan yang aman, skalabel, dan tangguh. Hasil evaluasi menunjukkan keselarasan arsitektur dengan prinsip NIST SP 800-207 Zero Trust *Architecture*, mitigasi risiko pada OWASP API *Security Top* 10, serta dukungan terhadap kebutuhan kepatuhan PCI DSS dan ISO/IEC 27001. Model yang dihasilkan dapat menjadi referensi dalam pengembangan platform Digital Banking yang aman dan adaptif.

Korespondensi Penulis:

B. Junedi Hutagaol,
Universitas Asa Indonesia, Jakarta Timur
Telepon : +6281294085438
Email: *junedi@asaindo.ac.id*

Submitted : 17-06-2026; Accepted : 11-08-2026;

Published : 11-08-2026

1. PENDAHULUAN

Perkembangan perbankan digital telah mengubah cara lembaga keuangan merancang dan mengoperasikan platform teknologinya. Sistem perbankan modern semakin bergantung pada platform digital untuk mendukung berbagai layanan, seperti *mobile banking, open banking*, pembayaran digital, dan transaksi keuangan secara *real-time*

[1]. Transformasi ini secara signifikan meningkatkan kebutuhan akan infrastruktur teknologi informasi yang memiliki ketersediaan tinggi, aman, dan skalabel guna mendukung penyediaan layanan secara berkelanjutan serta integrasi yang mulus dengan mitra eksternal [2]. Seiring semakin terhubungnya ekosistem perbankan, *Application Programming Interface* (API) telah menjadi komponen penting dalam mendorong inovasi digital dengan memfasilitasi komunikasi antara sistem internal perbankan, *platform financial technology (fintech)*, penyedia layanan pihak ketiga, dan infrastruktur regulator [3].

API Gateway berfungsi sebagai titik kendali arsitektural yang mengelola interaksi antara konsumen layanan, layanan internal, dan mitra eksternal dalam sistem perbankan modern [4]. *API Gateway* bertindak sebagai pintu masuk utama lalu lintas API serta menyediakan berbagai fungsi penting, seperti autentikasi, otorisasi, manajemen lalu lintas, *load balancing*, pemantauan, pembatasan laju akses (*rate limiting*), dan orkestrasi layanan. Dalam lingkungan perbankan digital, *API Gateway* tidak hanya bertanggung jawab mengelola komunikasi antara klien dan layanan *backend*, tetapi juga menerapkan mekanisme pengamanan serta menjamin keandalan layanan [5]. Oleh karena itu, desain arsitektur *API Gateway* memiliki pengaruh langsung terhadap kinerja sistem, ketahanan operasional, dan kepatuhan terhadap persyaratan regulasi [6].

Meskipun integrasi berbasis API memberikan berbagai manfaat, meningkatnya eksposur layanan perbankan melalui API juga menghadirkan tantangan keamanan yang signifikan [7]. Semakin terbukanya API perbankan terhadap interaksi eksternal memperluas permukaan serangan (*attack surface*) pada sistem keuangan. Berbagai risiko keamanan, seperti eksploitasi API oleh pihak yang tidak berwenang, kompromi kredensial pengguna, upaya gangguan layanan, serangan berbasis injeksi, dan aktivitas akses ilegal, mengharuskan institusi keuangan memperkuat arsitektur keamanan serta mekanisme tata kelolanya [8]. Berdasarkan berbagai laporan industri terkini, Selain kesadaran pengguna akan keamanan digital [9], API telah menjadi salah satu sasaran utama serangan siber pada infrastruktur digital modern karena menyediakan akses langsung terhadap fungsi bisnis yang sensitif dan data nasabah [10]. Pendekatan keamanan tradisional yang berorientasi pada perimeter jaringan semakin tidak memadai dalam menghadapi ancaman tersebut karena masih mengandalkan asumsi kepercayaan implisit setelah pengguna atau sistem berhasil memasuki jaringan.

Kompleksitas ekosistem perbankan digital yang terus meningkat menuntut pendekatan keamanan yang mampu beroperasi melampaui batas-batas jaringan tradisional. Oleh karena itu, *Zero Trust Architecture* (ZTA) diperkenalkan sebagai model arsitektur keamanan yang menghilangkan asumsi kepercayaan implisit melalui penerapan proses verifikasi berkelanjutan dan pengambilan keputusan akses berdasarkan kebijakan (*policy-based access control*). Dalam pendekatan ini, setiap interaksi terhadap layanan perbankan dievaluasi berdasarkan identitas, konteks otorisasi, dan kondisi keamanan sebelum akses diberikan [11], [12]. Penerapan prinsip-prinsip ZTA telah direkomendasikan untuk sektor-sektor kritis, termasuk sektor jasa keuangan, karena mampu menyediakan kerangka keamanan yang lebih kuat dalam menghadapi ancaman siber yang semakin kompleks [13]. Integrasi kapabilitas ZTA ke dalam arsitektur API Gateway dapat memperkuat mekanisme pengendalian akses, mengurangi permukaan serangan, serta meningkatkan visibilitas pada lingkungan perbankan yang terdistribusi [11].

Selain aspek keamanan, institusi keuangan juga harus menyeimbangkan kebutuhan akan penyediaan layanan digital yang lebih cepat dan skalabilitas infrastruktur dengan kewajiban tata kelola yang ditetapkan oleh berbagai regulasi [14]. Platform *public cloud* menawarkan elastisitas, penyediaan sumber daya yang cepat, serta efisiensi biaya sehingga menjadi pilihan menarik untuk mendukung beban kerja (*workload*) perbankan digital [6], [15]. Namun demikian, persyaratan regulasi terkait kedaulatan data (*data sovereignty*), perlindungan privasi, dan pengendalian operasional sering kali menghambat bank untuk memigrasikan seluruh beban kerja kritis ke lingkungan *public cloud*. Oleh sebab itu, banyak institusi keuangan masih mempertahankan infrastruktur *private cloud* maupun *on-premises* untuk mengelola aplikasi yang bersifat sensitif dan data nasabah [16].

Arsitektur *hybrid cloud* muncul sebagai solusi yang menjanjikan dalam menyeimbangkan kebutuhan-kebutuhan tersebut. Dengan mengombinasikan lingkungan *private cloud* atau *on-premises* dengan layanan *public cloud, hybrid cloud* memungkinkan institusi keuangan tetap mempertahankan kendali atas aset-aset kritis sekaligus memanfaatkan skalabilitas dan fleksibilitas *cloud* untuk beban kerja yang tidak sensitif [17]. Pendekatan *API Gateway* pada lingkungan *hybrid cloud* mampu meningkatkan ketahanan sistem, mendukung distribusi beban kerja, menyediakan skalabilitas dinamis, serta memperbaiki kemampuan pemulihan bencana (*disaster recovery*) [17], [18]. Arsitektur ini memungkinkan bank mengoptimalkan pemanfaatan infrastruktur tanpa mengabaikan persyaratan keamanan dan kepatuhan yang ketat.

Meskipun demikian, perancangan arsitektur *API Gateway* pada lingkungan *hybrid cloud* menghadapi berbagai tantangan. Arsitektur tersebut harus mampu menjamin komunikasi yang aman pada lingkungan yang heterogen, menerapkan kebijakan pengendalian akses secara konsisten, memenuhi ketentuan regulasi, serta mendukung penskalaan elastis ketika terjadi lonjakan jumlah transaksi [19]. Dalam lingkungan perbankan digital, persyaratan arsitektural tersebut menjadi sangat penting karena kegagalan dalam menjaga ketersediaan layanan, kinerja sistem, maupun keamanan dapat secara langsung memengaruhi keberlangsungan bisnis, kepercayaan nasabah, serta kepatuhan terhadap regulasi industri keuangan [11], [20].

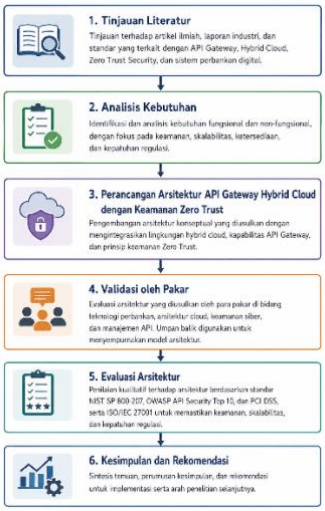
Berbagai penelitian sebelumnya umumnya berfokus pada mekanisme keamanan *API Gateway* [21], manajemen API berbasis *cloud* [22], atau implementasi ZTA [23], [24] sebagai domain penelitian yang terpisah. Demikian pula, sebagian besar penelitian mengenai arsitektur *cloud* hanya membahas implementasi pada *private*

cloud maupun *public cloud* secara terpisah [2]. Penelitian yang mengintegrasikan arsitektur *hybrid cloud*, teknologi *API Gateway*, dan prinsip keamanan ZTA ke dalam suatu kerangka arsitektur terpadu yang secara khusus dirancang untuk sistem perbankan digital masih sangat terbatas. Selain itu, literatur yang ada juga masih jarang membahas tantangan ganda dalam mewujudkan jaminan keamanan yang kuat sekaligus penyediaan layanan yang skalabel pada lingkungan *hybrid cloud* untuk sektor perbankan. Kesenjangan penelitian ini menunjukkan perlunya suatu rancangan arsitektur yang mampu mengintegrasikan seluruh aspek tersebut ke dalam sebuah kerangka kerja yang komprehensif.

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan Arsitektur *API Gateway Hybrid Cloud* berbasis *Zero Trust* untuk sistem perbankan digital. Arsitektur yang diusulkan bertujuan menyediakan kerangka konseptual yang mampu meningkatkan keamanan, skalabilitas, fleksibilitas operasional, serta kepatuhan terhadap regulasi. Dengan mengintegrasikan mekanisme pengendalian ZTA ke dalam model implementasi *hybrid cloud*, arsitektur ini berupaya memastikan proses verifikasi berkelanjutan terhadap setiap permintaan akses sekaligus mendukung penskalaan beban kerja secara dinamis pada lingkungan yang terdistribusi. Penelitian ini menawarkan suatu kerangka arsitektur terpadu yang mengombinasikan konsep *Hybrid Cloud, API Gateway*, dan *Zero Trust* guna mendukung pengembangan infrastruktur perbankan digital yang aman, skalabel, dan tangguh. Kerangka kerja yang diusulkan diharapkan dapat menjadi acuan praktis bagi institusi perbankan maupun praktisi teknologi dalam membangun ekosistem berbasis API yang memenuhi kebutuhan keamanan, skalabilitas, serta tata kelola.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi *Design Science Research* (DSR) dengan pendekatan kualitatif untuk merancang Arsitektur *API Gateway Hybrid Cloud* berbasis prinsip ZTA pada lingkungan perbankan digital. Metodologi DSR dipilih sebagai kerangka penelitian untuk memandu proses pengembangan dan evaluasi artefak arsitektur yang diusulkan dalam menjawab tantangan terkait keamanan, skalabilitas, dan kepatuhan terhadap regulasi. Artefak yang dihasilkan berupa arsitektur konseptual yang mengintegrasikan mekanisme keamanan, strategi implementasi *cloud*, serta kebutuhan tata kelola. Proses penelitian dilaksanakan melalui enam tahapan, sebagaimana ditunjukkan pada Gambar 1.



Gambar 1 : Metode Penelitian

Tinjauan Literature

Tahap pertama dilakukan melalui kajian literatur secara komprehensif terhadap publikasi ilmiah, laporan industri, dan standar internasional yang berkaitan dengan teknologi *API Gateway, Hybrid Cloud Computing, Zero Trust Architecture* (ZTA), dan sistem perbankan digital. Tahap ini bertujuan untuk membangun landasan teoretis penelitian, mengidentifikasi tantangan terkini pada infrastruktur perbankan berbasis API, serta mengkaji praktik terbaik dalam penerapan arsitektur yang aman dan skalabel. Hasil kajian literatur menjadi dasar pengetahuan utama yang digunakan pada tahapan penelitian selanjutnya.

Analisis Kebutuhan

Tahap kedua berfokus pada identifikasi kebutuhan arsitektural dalam implementasi *API Gateway* pada sistem perbankan digital. Analisis dilakukan dengan mempertimbangkan aspek-aspek utama, seperti keamanan, skalabilitas, ketersediaan layanan (*availability*), dan kepatuhan terhadap regulasi. Perhatian khusus diberikan pada tantangan yang dihadapi institusi keuangan dalam menyeimbangkan kebutuhan keamanan yang ketat dengan tuntutan kelincahan operasional (*operational agility*) serta adopsi teknologi *cloud*. Luaran dari tahap ini adalah seperangkat kebutuhan arsitektural yang menjadi acuan dalam perancangan solusi yang diusulkan.

Perancangan Arsitektur API Gateway Hybrid Cloud Berbasis Zero Trust

Berdasarkan kebutuhan yang telah diidentifikasi, dikembangkan sebuah arsitektur konseptual yang mengintegrasikan infrastruktur *Hybrid Cloud*, kapabilitas *API Gateway*, dan prinsip keamanan ZTA. Arsitektur yang

diusulkan dirancang untuk mendukung komunikasi yang aman antara aplikasi perbankan, mitra eksternal, dan layanan *cloud* dengan tetap memenuhi persyaratan regulasi. Mekanisme ZTA, seperti autentikasi berkelanjutan (*continuous authentication*), otorisasi, verifikasi identitas, enkripsi, dan penegakan kebijakan (*policy enforcement*), diintegrasikan ke dalam arsitektur untuk memastikan bahwa setiap permintaan akses divalidasi tanpa bergantung pada asal permintaan tersebut. Selain itu, rancangan ini juga mendefinisikan mekanisme interaksi antara lingkungan *private cloud* dan *public cloud* guna mencapai skalabilitas serta ketahanan operasional yang optimal.

Validasi oleh Pakar

Tahap keempat berfokus pada peninjauan arsitektur yang diusulkan melalui proses validasi oleh pakar. Pakar yang berasal dari bidang teknologi perbankan, arsitektur cloud, keamanan siber, dan manajemen API mengevaluasi model yang diusulkan untuk menilai kesesuaian, kelengkapan, dan kemudahan penerapannya dalam praktik. Masukan yang diperoleh dari proses evaluasi digunakan sebagai dasar penyempurnaan rancangan arsitektur sebelum dilakukan penilaian akhir.

Evaluasi Arsitektur

Tahap kelima bertujuan untuk mengevaluasi arsitektur yang diusulkan menggunakan pendekatan penilaian kualitatif. Evaluasi difokuskan pada sejauh mana arsitektur mampu memenuhi kebutuhan keamanan, skalabilitas, dan kepatuhan yang telah diidentifikasi pada tahap sebelumnya. Aspek keamanan dievaluasi dengan mengacu pada prinsip-prinsip yang terdapat dalam NIST SP 800-207 dan kerangka kerja OWASP *API Security Top* 10, sedangkan aspek kepatuhan dianalisis berdasarkan standar PCI DSS dan ISO/IEC 27001. Selain itu, evaluasi juga menilai kemampuan arsitektur dalam mendukung skalabilitas beban kerja (*workload scalability*), pengelolaan lalu lintas (*traffic management*), dan ketersediaan layanan yang tinggi (*high availability*) pada lingkungan *hybrid cloud*.

Kesimpulan dan Rekomendasi

Tahap terakhir merupakan proses sintesis terhadap seluruh hasil yang diperoleh dari tahapan perancangan, validasi, dan evaluasi. Berdasarkan hasil tersebut, disusun kesimpulan mengenai kesesuaian Arsitektur *API Gateway Hybrid Cloud* Berbasis *Zero Trust* untuk diterapkan pada sistem perbankan digital. Selanjutnya, disampaikan rekomendasi bagi institusi perbankan yang berencana mengadopsi lingkungan *hybrid cloud* dan infrastruktur API berbasis ZTA. Selain itu, penelitian ini juga mengidentifikasi arah penelitian lanjutan, seperti implementasi prototipe, pengujian kinerja, dan validasi empiris pada lingkungan operasional perbankan..

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil perancangan dan evaluasi terhadap Arsitektur *API Gateway Hybrid Cl*oud Berbasis *Zero Trust* yang diusulkan. Analisis difokuskan pada empat aspek utama, yaitu perancangan arsitektur, implementasi *Zero Trust*, implementasi *Hybrid Cloud*, serta evaluasi kepatuhan terhadap standar keamanan yang telah ditetapkan.

Analisis Kebutuhan Sistem Perbankan Digital

Hasil kajian literatur dan analisis kebutuhan menunjukkan bahwa sistem perbankan digital modern menghadapi tuntutan yang semakin tinggi terhadap penyediaan layanan yang aman, skalabel, dan memiliki ketersediaan tinggi (*high availability*). Meningkatnya adopsi *mobile banking*, platform pembayaran digital, inisiatif *open banking*, serta integrasi dengan perusahaan *financial technology* (*fintech*) telah menyebabkan peningkatan volume lalu lintas API dan kompleksitas interaksi antar layanan.

Seiring berkembangnya layanan perbankan menuju ekosistem berbasis API, semakin banyaknya integrasi dengan aplikasi internal, penyedia layanan pihak ketiga, dan berbagai kanal digital turut meningkatkan kompleksitas pengelolaan keamanan. Paparan API (*API exposure*) menimbulkan berbagai potensi risiko, seperti penyalahgunaan identitas, akses tidak sah, pemanggilan API yang bersifat malicious, serta gangguan terhadap ketersediaan layanan. Oleh karena itu, pendekatan keamanan tradisional yang hanya mengandalkan perlindungan pada perimeter jaringan (*perimeter-based security*) tidak lagi memadai. Keputusan pemberian akses harus didasarkan pada proses verifikasi berkelanjutan (*continuous verification*), bukan semata-mata berdasarkan lokasi jaringan [25], [26], [27].

Selain aspek keamanan, institusi perbankan juga harus memenuhi berbagai persyaratan regulasi yang ketat terkait perlindungan data nasabah, kemampuan audit (*auditability*), dan ketahanan operasional (*operational resilience*). Persyaratan tersebut sering kali membatasi migrasi penuh beban kerja (*workload*) yang bersifat kritis ke lingkungan *public cloud*. Oleh karena itu, banyak institusi keuangan mengadopsi strategi *hybrid cloud* untuk menyeimbangkan kepatuhan terhadap regulasi dengan manfaat skalabilitas yang ditawarkan oleh teknologi *cloud*.

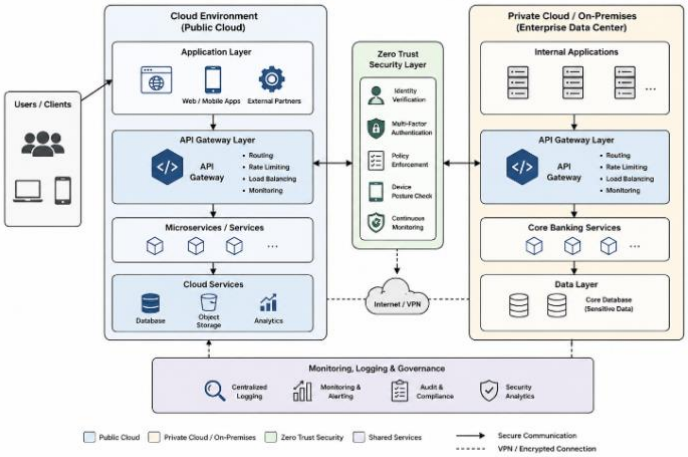
Berdasarkan hasil analisis, terdapat empat kebutuhan arsitektural utama yang menjadi dasar dalam perancangan solusi, yaitu:

1. Keamanan yang kuat melalui mekanisme verifikasi berkelanjutan (*continuous verification*) dan pengendalian akses (*access control*).
2. Skalabilitas elastis (*elastic scalability*) untuk mendukung fluktuasi volume transaksi.
3. Ketersediaan layanan yang tinggi (*high availability*) dan ketahanan (*resilience*) bagi layanan perbankan yang bersifat *mission-critical*.
4. Dukungan terhadap kepatuhan regulasi (*regulatory compliance*) dan tata kelola data (*data governance*).

Keempat kebutuhan tersebut menjadi landasan utama dalam pengembangan arsitektur yang diusulkan.

Arsitektur *API Gateway Hybrid Cloud* yang Diusulkan

Hasil kajian literatur dan analisis kebutuhan menunjukkan bahwa sistem perbankan digital modern menghadapi tuntutan yang semakin tinggi terhadap penyediaan layanan yang aman, skalabel, dan memiliki ketersediaan tinggi (*high availability*) [2], [12], [21], [27], [28]. Meningkatnya adopsi *mobile banking*, platform pembayaran digital, inisiatif *open banking*, serta integrasi dengan perusahaan *financial technology* (*fintech*) telah menyebabkan peningkatan volume lalu lintas API dan kompleksitas interaksi antar layanan [29], [30], [31].



Gambar 2: Arsitektur API Gateway Hybrid Cloud

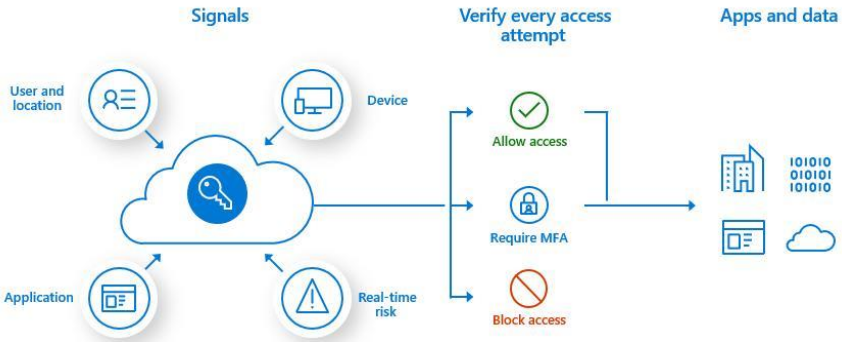
Arsitektur yang diusulkan terdiri atas enam lapisan yang saling terintegrasi, yaitu:

1. Lapisan Akses Klien (*Client Access Layer*), yang mencakup aplikasi *mobile banking*, portal *internet banking*, aplikasi *fintech* mitra, serta sistem internal perbankan yang mengonsumsi layanan API.
2. Lapisan Keamanan *Zero Trust* (*ZTA Security Layer*), yang bertugas melakukan verifikasi identitas, autentikasi multifaktor (*Multi-Factor Authentication*/*MFA*), validasi perangkat, otorisasi berkelanjutan (*continuous authorization*), dan penerapan kebijakan keamanan (*policy enforcement*) terhadap setiap permintaan API.
3. Lapisan API Gateway (*API Gateway Layer*), yang berfungsi sebagai titik masuk utama (*central entry point*) bagi seluruh lalu lintas API. Lapisan ini menyediakan berbagai fungsi, seperti *routing*, *rate limiting*, *load balancing*, orkestrasi API, pemantauan (*monitoring*), serta perlindungan terhadap ancaman (*threat protection*).
4. Lapisan Integrasi Layanan (*Service Integration Layer*), yang menghubungkan layanan *microservices*, sistem *core banking*, layanan pembayaran, dan integrasi dengan pihak ketiga melalui komunikasi API yang aman.
5. Lapisan Infrastruktur *Hybrid Cloud* (*Hybrid Cloud Infrastructure Layer*), yang mengombinasikan infrastruktur *private cloud* atau *on-premises* untuk menangani beban kerja (*workload*) perbankan yang bersifat sensitif dengan layanan *public cloud* untuk mendukung beban kerja yang skalabel dan tidak bersifat sensitif.
6. Lapisan Pemantauan dan Tata Kelola (*Monitoring and Governance Layer*), yang menyediakan pencatatan terpusat (*centralized logging*), analisis keamanan (*security analytics*), jejak audit (*audit trail*), pemantauan kepatuhan (*compliance monitoring*), serta tata kelola operasional (*operational governance*).

Rancangan arsitektur berlapis (*layered architecture*) ini memastikan bahwa seluruh mekanisme pengamanan diterapkan sebelum permintaan API diteruskan ke layanan *backend* perbankan. Selain itu, arsitektur ini memisahkan beban kerja yang bersifat sensitif dari beban kerja yang memanfaatkan skalabilitas *cloud*, sehingga memungkinkan institusi keuangan mengoptimalkan keamanan sekaligus meningkatkan efisiensi operasional.

Integrasi Prinsip Keamanan dengan ZTA

Arsitektur yang diusulkan mengintegrasikan prinsip-prinsip Zero Trust Architecture (ZTA) sebagai mekanisme keamanan utama pada lapisan API *Gateway*. Berbeda dengan pendekatan keamanan tradisional yang berorientasi pada perimeter jaringan dan membangun kepercayaan berdasarkan lokasi jaringan, model yang diusulkan menerapkan mekanisme verifikasi berkelanjutan (*continuous verification*) pada setiap interaksi antara pengguna, aplikasi, dan layanan perbankan. Pendekatan ini sangat relevan untuk lingkungan perbankan digital, di mana API menghubungkan berbagai entitas, termasuk sistem internal, mitra eksternal, platform *cloud*, dan pengguna yang tersebar di berbagai lokasi.



Gambar 3: Integrasi Prinsip Keamanan dengan ZTA

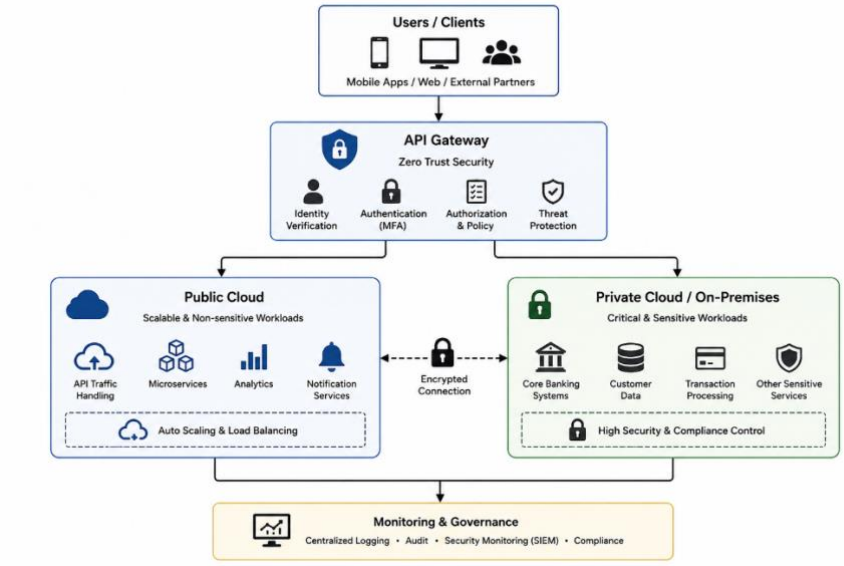
Dalam arsitektur yang diusulkan, API Gateway berfungsi sebagai lapisan penegakan kebijakan Zero Trust (*Zero Trust Enforcement Layer*) dengan melakukan evaluasi secara dinamis terhadap setiap permintaan akses sebelum komunikasi dengan layanan perbankan diizinkan. Proses pengambilan keputusan mempertimbangkan berbagai faktor keamanan, termasuk identitas pengguna, aturan otorisasi, status perangkat, dan konteks transaksi. Untuk aktivitas yang dikategorikan berisiko tinggi, diterapkan mekanisme verifikasi tambahan, seperti *Multi-Factor Authentication* (MFA), sedangkan kebijakan *Identity and Access Management* (IAM) menyediakan pengendalian terpusat terhadap hak akses di seluruh ekosistem perbankan.

Arsitektur yang diusulkan menempatkan API *Gateway* sebagai titik pengendalian *Zero Trust* melalui implementasi interaksi antara *Policy Enforcement Point* (PEP) dan *Policy Decision Point* (PDP). API *Gateway* bertanggung jawab untuk menegakkan keputusan akses, sedangkan PDP mengevaluasi atribut identitas, kebijakan keamanan, serta informasi kontekstual untuk menentukan apakah suatu permintaan akses diizinkan atau ditolak. Melalui pendekatan ini, proses otorisasi akses tidak lagi bersifat statis, tetapi menjadi proses evaluasi yang berkelanjutan sehingga mampu mendukung komunikasi API yang aman pada lingkungan perbankan berbasis *hybrid cloud*.

Integrasi Zero Trust Architecture (ZTA) juga meningkatkan kemampuan mitigasi terhadap berbagai ancaman pada API. Ancaman umum, seperti *credential stuffing*, akses tidak sah (*unauthorized access*), penyalahgunaan token (*token abuse*), dan serangan enumerasi API (*API enumeration attacks*), dapat diminimalkan melalui penerapan autentikasi adaptif (*adaptive authentication*), *rate limiting*, deteksi anomali (*anomaly detection*), serta kebijakan pengendalian akses yang ketat. Dengan demikian, arsitektur yang diusulkan mampu meningkatkan postur keamanan (*security posture*) sistem perbankan digital tanpa mengurangi kelancaran konektivitas layanan API.

Strategi Implementasi *Hybrid Cloud*

Hasil penting lainnya dari penelitian ini adalah perumusan strategi implementasi *hybrid cloud* yang dirancang khusus untuk lingkungan perbankan. Arsitektur yang diusulkan mengklasifikasikan beban kerja (*workload*) berdasarkan tingkat sensitivitas data dan persyaratan regulasi yang berlaku.



Gambar 4: Strategi Implementasi Hybrid Cloud

Rancangan *hybrid cloud* pada penelitian ini menerapkan strategi penempatan beban kerja (*workload placement*) dengan mendistribusikan komponen aplikasi berdasarkan klasifikasi keamanan, kewajiban kepatuhan (*compliance*), dan kebutuhan skalabilitas. Beban kerja perbankan yang bersifat sensitif, termasuk pemrosesan transaksi inti (*core transaction processing*) dan pengelolaan data nasabah, tetap ditempatkan pada lingkungan yang terkendali. Sementara itu, beban kerja yang membutuhkan elastisitas (*elastic workloads*) diimplementasikan pada platform *public cloud* untuk meningkatkan kelincahan operasional (*agility*) dan efisiensi pemanfaatan sumber daya. **API Gateway** berperan sebagai lapisan konektivitas terpadu yang menghubungkan kedua lingkungan tersebut dengan menerapkan komunikasi yang aman, pengendalian akses, dan pengelolaan lalu lintas (*traffic management*). Arsitektur ini memungkinkan sistem perbankan mencapai skalabilitas dan fleksibilitas operasional tanpa mengurangi efektivitas tata kelola keamanan.

Pendekatan *hybrid cloud* yang diusulkan memberikan beberapa keuntungan, yaitu:

1. Skalabilitas (*Scalability*): Sumber daya *public cloud* dapat ditingkatkan secara dinamis untuk mengakomodasi lonjakan volume transaksi.
2. Efisiensi Biaya (*Cost Efficiency*): Beban kerja yang tidak bersifat kritis dapat memanfaatkan model layanan *pay-as-you-go* sehingga penggunaan sumber daya menjadi lebih efisien.
3. Kepatuhan terhadap Regulasi (*Regulatory Compliance*): Data yang bersifat sensitif tetap berada di bawah kendali infrastruktur *private cloud* atau infrastruktur internal (*on-premises*) milik bank.
4. Ketahanan Operasional (*Operational Resilience*): Beban kerja dapat didistribusikan pada beberapa lingkungan sehingga meningkatkan kemampuan *disaster recovery* dan menjamin keberlangsungan layanan (*service continuity*).

Dengan demikian, strategi *hybrid cloud* yang diusulkan mampu menyeimbangkan kebutuhan akan kelincahan (*agility*) dan inovasi dengan tuntutan tata kelola serta kepatuhan yang ketat pada sektor perbankan.

Evaluasi terhadap Standar Keamanan dan Kepatuhan

Evaluasi terhadap arsitektur yang diusulkan dilakukan menggunakan pendekatan *framework-based qualitative evaluation* melalui teknik *architecture mapping.* Pada tahap ini, setiap komponen utama dalam arsitektur, seperti *Identity and Access Management* (IAM), *Multi-Factor Authentication* (MFA), *Policy Enforcement Point* (PEP), *Policy Decision Point* (PDP), *API Gateway, audit logging, monitoring*, serta mekanisme *Hybrid Cloud*, dipetakan dan dibandingkan dengan prinsip maupun kontrol keamanan yang terdapat pada NIST SP 800-207, OWASP API Security Top 10, PCI DSS, dan ISO/IEC 27001. Proses pemetaan dilakukan untuk menilai sejauh mana komponen-komponen arsitektur telah memenuhi kebutuhan keamanan, pengendalian akses, perlindungan API, kepatuhan terhadap regulasi, dan tata kelola data pada lingkungan perbankan digital. Hasil evaluasi menunjukkan bahwa arsitektur yang diusulkan memiliki tingkat kesesuaian yang tinggi dengan standar internasional dan praktik terbaik yang direkomendasikan oleh keempat kerangka kerja tersebut.

Arsitektur yang diusulkan menunjukkan kesesuaian dengan berbagai kerangka kerja keamanan melalui integrasi mekanisme penegakan ZTA dan pengendalian keamanan API di dalam ekosistem perbankan. Implementasi keputusan akses berbasis identitas (*identity-based access decisions*), evaluasi berkelanjutan terhadap setiap permintaan (*continuous request evaluation*), serta otorisasi berbasis kebijakan (*policy-driven authorization*) mengurangi ketergantungan pada model keamanan tradisional yang berorientasi pada perimeter jaringan. Selain itu, arsitektur ini menerapkan mekanisme pengendalian preventif (*preventive controls*) dan detektif (*detective controls*) untuk mengatasi berbagai ancaman terhadap API, seperti akses tidak sah (*unauthorized access*), konsumsi sumber daya yang berlebihan (*excessive resource consumption*), permintaan berbahaya (*malicious requests*), dan perilaku layanan yang tidak normal (*abnormal service behavior*). Kapabilitas tersebut memperkuat postur keamanan (*security posture*) platform perbankan digital yang beroperasi pada lingkungan *hybrid cloud*.

Dari perspektif kepatuhan (*compliance*), arsitektur yang diusulkan mendukung pemenuhan persyaratan PCI DSS, khususnya terkait transmisi data yang aman (*secure transmission*), pengendalian akses (*access control*), pencatatan jejak audit (*audit logging*), dan segmentasi jaringan (*network segmentation*). Selain itu, arsitektur ini juga selaras dengan kontrol keamanan yang ditetapkan dalam ISO/IEC 27001, terutama pada aspek manajemen keamanan informasi, penanganan risiko (*risk treatment*), dan keamanan operasional (*operational security*). Pemisahan beban kerja yang bersifat sensitif ke dalam lingkungan *private cloud* semakin memperkuat kepatuhan terhadap persyaratan tata kelola data (*data governance*) dan kedaulatan data (*data sovereignty*) yang berlaku di sektor perbankan.

Hasil Validasi Pakar

Validasi terhadap arsitektur yang diusulkan dilakukan melalui expert review dengan melibatkan tujuh orang pakar yang dipilih menggunakan teknik purposive sampling. Pemilihan pakar didasarkan pada kompetensi dan pengalaman di bidang *Enterprise Architecture, cloud computing*, keamanan siber , *API Management*, dan perbankan digital. Kriteria pakar meliputi memiliki pengalaman profesional minimal 10 tahun pada bidang terkait, pernah terlibat dalam perancangan, implementasi, atau pengelolaan arsitektur TI pada organisasi berskala enterprise atau institusi keuangan, serta memiliki peran sebagai *Enterprise Architect, Solution Architect, Cloud Architect, Security Architect*, dan *API Specialist* pada perbankan.

Proses validasi dilakukan melalui wawancara semi-terstruktur dan penelaahan dokumen arsitektur. Setiap pakar diberikan dokumen rancangan Arsitektur API *Gateway Hybrid Cloud* beserta penjelasan mengenai fungsi setiap komponen. Selanjutnya, para pakar diminta melakukan penilaian terhadap lima aspek utama, yaitu efektivitas keamanan, dukungan skalabilitas, kelengkapan arsitektur, kelayakan operasional, dan kepatuhan terhadap regulasi. Selain memberikan penilaian, para pakar juga menyampaikan masukan dan rekomendasi untuk penyempurnaan rancangan arsitektur.

Hasil validasi menunjukkan bahwa secara umum para pakar menilai arsitektur yang diusulkan telah menyediakan kerangka kerja yang komprehensif dalam mendukung implementasi API *Gateway* berbasis *Hybrid Cloud* dengan pendekatan *Zero Trust*. Integrasi antara API *Gateway*, mekanisme ZTA, serta strategi *Hybrid Cloud* dinilai mampu meningkatkan keamanan komunikasi API tanpa mengurangi kebutuhan skalabilitas dan fleksibilitas operasional pada lingkungan perbankan digital.

Para pakar mengevaluasi arsitektur berdasarkan lima kriteria utama, yaitu efektivitas keamanan, kemampuan skalabilitas, kelengkapan arsitektur, kelayakan operasional, dan kepatuhan terhadap regulasi. Secara umum, para evaluator menyatakan bahwa arsitektur yang diusulkan menyediakan kerangka kerja yang komprehensif untuk mengamankan layanan perbankan berbasis API sekaligus mendukung strategi implementasi *hybrid cloud*.

Beberapa rekomendasi diperoleh selama proses validasi. Pertama, para pakar merekomendasikan penerapan *Identity and Access Management* (IAM) yang terpusat untuk memastikan pengendalian akses yang konsisten pada lingkungan *private cloud* maupun *public cloud*. Kedua, mekanisme pemantauan berkelanjutan (*continuous monitoring*) dan analitik keamanan (*security analytics*) perlu diintegrasikan guna meningkatkan kemampuan deteksi terhadap ancaman. Ketiga, lalu lintas API perlu dilindungi melalui mekanisme *rate limiting* yang lebih canggih serta analisis perilaku (*behavioral analysis*) untuk memitigasi berbagai serangan API yang terus berkembang. Seluruh rekomendasi tersebut telah diakomodasi dalam penyempurnaan versi akhir arsitektur yang diusulkan. Ringkasan hasil validasi pakar disajikan pada Tabel 1.

.

Tabel 1: Ringkasan Hasil Validasi Pakar

Aspek Evaluasi	Kriteria Assessment	Hasil	Justifikasi
Efektivitas Keamanan	Implementasi kontrol ZTA, IAM, MFA, PEP, PDP, policy enforcement	Tinggi	Seluruh mekanisme utama Zero Trust telah terimplementasi sehingga mampu meningkatkan pengendalian akses API.
Dukungan Skalabilitas	Kemampuan Hybrid Cloud mendukung elastisitas workload dan distribusi layanan	Tinggi	Mendukung autoscaling, load balancing, dan distribusi workload pada private dan public cloud.
Kelengkapan Arsitektur	Kelengkapan komponen utama API Gateway Hybrid Cloud	Tinggi	Seluruh komponen utama arsitektur telah direpresentasikan.
Kelayakan Operasional	Kemudahan implementasi pada lingkungan perbankan	Sedang–Tinggi	Memerlukan penyesuaian terhadap infrastruktur dan proses operasional yang telah ada.
Kepatuhan Regulasi	Kesesuaian terhadap PCI DSS, ISO/IEC 27001, dan prinsip Zero Trust	Tinggi	Mendukung kontrol keamanan dan tata kelola yang direkomendasikan oleh framework terkait.

Pembahasan

Hasil penelitian menunjukkan bahwa integrasi *Hybrid Cloud, API Gateway,* dan ZTA ke dalam suatu kerangka arsitektur terpadu mampu memberikan pendekatan yang lebih komprehensif dalam mendukung transformasi digital pada sektor perbankan. Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa implementasi API *Gateway* tidak lagi hanya berfungsi sebagai mekanisme *traffic management* dan integrasi layanan, tetapi telah berkembang menjadi komponen utama dalam penerapan kebijakan keamanan, pengelolaan identitas, dan pengendalian akses pada arsitektur berbasis layanan (*service-oriented* maupun *microservices architecture*) [4], [19], [20]. Dengan mengintegrasikan fungsi keamanan secara langsung pada API Gateway, arsitektur yang diusulkan mampu memperkuat perlindungan terhadap layanan API tanpa menambah kompleksitas pada sisi aplikasi.

Dari perspektif keamanan, hasil penelitian ini juga mendukung konsep ZTA yang diperkenalkan dalam NIST SP 800-207, yang menekankan bahwa tidak ada entitas yang secara otomatis dipercaya, baik yang berasal dari jaringan internal maupun eksternal. Prinsip *continuous verification, least privilege access,* serta *policy-based access control* yang diimplementasikan pada arsitektur yang diusulkan selaras dengan rekomendasi NIST dalam membangun sistem yang mampu menghadapi lingkungan komputasi modern yang semakin terdistribusi. Selain itu, penerapan Identity and IAM, PDP, dan PEP memperkuat mekanisme pengambilan keputusan akses secara dinamis berdasarkan identitas, konteks, dan kebijakan keamanan yang berlaku.

Strategi *Hybrid Cloud* yang diusulkan juga memperkuat temuan penelitian terdahulu yang menyatakan bahwa institusi keuangan memerlukan keseimbangan antara fleksibilitas komputasi awan dan kepatuhan terhadap regulasi. Penempatan beban kerja (*workload placement*) berdasarkan tingkat sensitivitas data memungkinkan layanan

yang bersifat kritis tetap dijalankan pada lingkungan *private cloud*, sedangkan layanan yang membutuhkan elastisitas memanfaatkan public cloud. Pendekatan ini sejalan dengan praktik terbaik implementasi hybrid cloud pada sektor keuangan yang bertujuan menjaga keamanan data sekaligus meningkatkan skalabilitas dan efisiensi operasional [19], [32].

Selain itu, hasil evaluasi menunjukkan bahwa arsitektur yang diusulkan memiliki kesesuaian dengan berbagai standar keamanan, termasuk NIST SP 800-207, OWASP API Security Top 10, PCI DSS, dan ISO/IEC 27001. Kesesuaian tersebut menunjukkan bahwa rancangan arsitektur tidak hanya memenuhi kebutuhan teknis dalam pengamanan layanan API, tetapi juga mendukung penerapan tata kelola keamanan informasi yang menjadi persyaratan penting pada industri perbankan digital. Temuan ini memperkuat penelitian sebelumnya yang menyatakan bahwa integrasi antara kontrol keamanan API dan tata kelola keamanan informasi merupakan faktor penting dalam meningkatkan ketahanan (*cyber resilience*) sistem perbankan berbasis *cloud* [33], [34].

Kontribusi utama penelitian ini dibandingkan penelitian terdahulu terletak pada penyusunan sebuah kerangka arsitektur terpadu yang mengintegrasikan tiga komponen utama, yaitu *Hybrid Cloud, API Gateway*, dan ZTA, dalam satu model konseptual untuk lingkungan perbankan digital. Sebagian besar penelitian sebelumnya membahas ketiga aspek tersebut secara terpisah, sedangkan penelitian ini menunjukkan bagaimana ketiganya dapat diintegrasikan untuk mendukung keamanan, skalabilitas, serta kepatuhan terhadap regulasi dalam satu rancangan arsitektur yang utuh.

Meskipun demikian, penelitian ini masih memiliki beberapa keterbatasan. Arsitektur yang diusulkan masih bersifat konseptual dan belum diimplementasikan pada lingkungan operasional perbankan (*production environment*). Oleh karena itu, aspek yang bersifat kuantitatif, seperti *latency, throughput, resource utilization*, dan biaya operasional, belum dapat dievaluasi secara empiris. Penelitian selanjutnya disarankan untuk mengembangkan prototipe, melakukan simulasi maupun studi kasus pada lingkungan perbankan yang sesungguhnya sehingga efektivitas arsitektur dapat divalidasi melalui pengukuran kinerja dan pengujian keamanan secara lebih komprehensif.

4. KESIMPULAN

Penelitian ini berhasil mengusulkan Arsitektur API *Gateway Hybrid Cloud* berbasis ZTA untuk mendukung keamanan, skalabilitas, dan kepatuhan pada sistem perbankan digital dengan menggunakan metodologi *Design Science Research* (DSR). Melalui tahapan identifikasi kebutuhan, perancangan, validasi pakar, dan evaluasi terhadap standar keamanan, penelitian ini menghasilkan sebuah model arsitektur konseptual yang mengintegrasikan kapabilitas API *Gateway, Hybrid Cloud,* dan prinsip-prinsip *Zero Trust* dalam satu kerangka yang terpadu.

Hasil validasi pakar dan evaluasi menunjukkan bahwa arsitektur yang diusulkan memiliki kesesuaian dengan prinsip NIST SP 800-207, OWASP API *Security Top* 10, serta mendukung kontrol keamanan yang direkomendasikan dalam PCI DSS dan ISO/IEC 27001. Temuan ini menunjukkan bahwa arsitektur yang diusulkan layak dijadikan sebagai referensi konseptual dalam pengembangan platform perbankan digital yang aman dan adaptif.

Kontribusi utama penelitian ini terletak pada penyusunan model arsitektur yang mengintegrasikan *Hybrid Cloud, API Gateway*, dan ZTA, yang pada penelitian-penelitian sebelumnya umumnya masih dibahas secara terpisah. Dengan demikian, penelitian ini memberikan kontribusi baik secara akademis maupun praktis sebagai acuan dalam perancangan arsitektur perbankan digital yang mendukung keamanan, skalabilitas, dan kepatuhan terhadap regulasi.

Penelitian ini masih terbatas pada tahap perancangan dan evaluasi konseptual sehingga belum dilakukan implementasi maupun pengujian pada lingkungan operasional perbankan. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan prototipe, melakukan pengujian kinerja dan keamanan, serta mengevaluasi implementasi arsitektur pada studi kasus nyata agar manfaat dan efektivitas model yang diusulkan dapat dibuktikan secara empiris.

REFERENCES

[1] M. Hamed, M. Hefny, Y. Helmy, and M. Abdelsalam, “Open Banking API Framework to Improve the Online Transaction between Local Banks in Egypt Using Blockchain Technology,” vol. 14, no. 4, 2023, doi: 10.12720/jait.14.4.729-740.

[2] Vedaswaroop Meduri, “Hybrid Cloud Architectures for Scalable and Cost-Effective AI in Banking,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 1840–1849, 2024, doi: 10.32628/cseit241061226.

[3] G. B. Navaretti, G. Calzolari, J. M. Mansilla-fernández, and A. F. Pozzolo, “Open Banking ’ s Promise of a Financial Revolution : Are We Falling Short ? 1 Open Banking ’ s Promise of a Financial Revolution : Are,” pp. 1–21, 2022.

[4] Z. Butcher and Z. Butcher, “NIST Special Publication 800 Guidelines for API Protection for Cloud-Native Systems Guidelines for API Protection for Cloud-Native Systems”.

[5] R. S. Sitorus *et al.*, “Capability-Based API Gateway Technology Selection Analysis for Banking Cybersecurity Solution Using AHP Method,” vol. 9, no. 1, pp. 338–347, 2025.

[6] O. Access, A. Katari, A. Muthsyala, and H. Allam, “Hybrid Cloud Architectures for Financial Data Lakes: Design Patterns and Use Cases,” *Int. Res. J. Mod. Eng. Technol. Sci.*, no. 01, pp. 1421–1430, 2024, doi: 10.56726/irjmets5966.

[7] P. Ranjan and S. Dahiya, “International Journal of Communication Networks and Information Security

Advanced Threat Detection in API Security: Leveraging Machine Learning Algorithms," *Int. J. Commun. Networks Inf. Secur.*, vol. 13, no. 1, 2021, [Online]. Available: https://ijcnis.org/
[8] Muhammad Sohail, "Intelligent threat detection and prevention in REST APIs using machine learning," *Int. J. Sci. Res. Arch.*, vol. 15, no. 2, pp. 012–027, 2025, doi: 10.30574/ijsra.2025.15.2.1281.
[9] B. J. Hutagaol, R. S. Sitorus, and N. Hutagaol, "Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman Cybercrime," *J. Teknol. Sist. Inf. dan Apl.*, vol. 7, no. 3, pp. 1043–1054, 2024, doi: 10.32493/jtsi.v7i3.41639.
[10] D. Jaiswal, "Zero-Trust Architecture for Telecom API Security: A Framework for the Communications Economy," *Eur. Mod. Stud. J.*, vol. 9, no. 4, pp. 11–21, 2025, doi: 10.59573/emsj.9(4).2025.2.
[11] R. S. Sitorus and B. J. Hutagaol, "Designing a Zero Trust Architecture for Securing API Gateways in Digital Banking Systems," vol. 7, no. 3, pp. 2589–2601, 2025, doi: 10.51519/journalisi.v7i3.1219.
[12] Oluomachi Eunice Ejiofor, Oluwafemi Olusoga, and Ahmed Akinsola, "Zero trust architecture: A paradigm shift in network security," *Comput. Sci. IT Res. J.*, vol. 6, no. 3, pp. 104–124, 2025, doi: 10.51594/csitrj.v6i3.1871.
[13] S. Purella, "Zero-Trust Architecture in Distributed Financial Ecosystems," *Int. J. Comput. Eng.*, vol. 7, no. 20, pp. 11–26, 2025, doi: 10.47941/ijce.3075.
[14] Manvitha Potluri, "Secure DevSecOps for financial compliance: Building compliant cloud-native pipelines," *World J. Adv. Res. Rev.*, vol. 26, no. 2, pp. 324–333, 2025, doi: 10.30574/wjarr.2025.26.2.1618.
[15] S. Dai, "Banking Business in Digital Transformation: The Role of Cloud Computing," *J. Prog. Eng. Phys. Sci.*, vol. 3, no. 4, pp. 76–83, 2024, doi: 10.56397/jpeps.2024.12.11.
[16] Aditya Sharma, "Compliance and Regulatory Challenges in Cloud Adoption for Financial Services: A Comprehensive Analysis," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 5, pp. 505–515, 2025, doi: 10.32996/jcsts.2025.7.5.57.
[17] A. Meshram, "Hybrid Cloud Strategy for Mission-Critical Financial Software Applications," *Ijarcce*, vol. 14, no. 12, pp. 987–992, 2025, doi: 10.17148/ijarcce.2025.1412136.
[18] R. T. Natarajan, "Journal of Artificial Intelligence , Machine Learning and Data Science AI & Machine Learning in Applications Security and Vulnerability," pp. 1–4, 2024.
[19] V. Punniyamoorthy *et al.*, "Secure and Governed API Gateway Architectures for Multi-Cluster Cloud Environments," *Arxiv*, 2025.
[20] R. S. Sitorus, B. J. Hutagaol, R. Triana, and I. Technology, "Cloud Native Zero Trust API Gateway Architecture for Digital Banking Systems," vol. 7, no. 1, pp. 255–268, 2026.
[21] Vaibhav Haribhau Khedkar, "The Transformative Impact of Artificial Intelligence and Machine Learning on Marketing Operations," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 176–182, 2024, doi: 10.32628/cseit24106166.
[22] Z. Samira *et al.*, "API management and cloud integration model for SMEs," 2024.
[23] N. F. Syed and S. W. Shah, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
[24] T. A. K. Manne, "Implementing Zero Trust Architecture in Multi-Cloud Environments," *Int. J. Comput. Eng.*, vol. 7, no. 3, pp. 74–82, 2025, doi: 10.47941/ijce.2753.
[25] S. Huy, S. Ang, M. Ho, and V. Balasubramaniam, "Securing API Ecosystems in Banking: A Critical Review of Cyber Risks, Control Frameworks, and Future Trends," *Jordanian J. Informatics Comput.*, vol. 2026, no. 1, pp. 25–37, 2026, doi: 10.63180/jjic.thestap.2026.1.3.
[26] O. Bajaber, "Towards Zero Trust Network Security via Programmable Data Planes," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 53, no. 3, pp. 36–39, 2026, doi: 10.1145/3788882.3788898.
[27] B. Nicoletti, "Cloud Computing in Financial Services," *Cloud Comput. Financ. Serv.*, no. 03, 2013, doi: 10.1057/9781137273642.
[28] A. Alhakim and S. Sofia, "Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia," *J. Komunitas Yust.*, vol. 4, no. 2, pp. 377–385, 2021, doi: 10.23887/jatayu.v4i2.38089.
[29] N. Karri, "Demystifying APIsation of Fintech: Transforming Financial Infrastructure through Interface Integration," *Int. J. Comput. Eng.*, vol. 7, no. 6, pp. 1–13, 2025, doi: 10.47941/ijce.2918.
[30] O. C. Edo, T. Tenebe, E. Etu, A. Ayuwu, J. Emakhu, and S. Adebiyi, "Zero Trust Architecture: Trend and Impacton Information Security," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 12, no. 7, pp. 140–147, 2022, doi: 10.46338/ijetae0722_15.
[31] J. U. Umavezi and B. Odukale, "API Development and Modelling: Streamlining Financial Technology Integration for Seamless Digital Transactions," *Int. J. Res. Publ. Rev.*, vol. 6, no. 1, pp. 1556–1573, 2025, doi: 10.55248/gengpi.6.0125.0328.
[32] Zulfa Qur'anisa, Mira Herawati, Lisvi Lisvi, Melinda Helmalia Putri, and O. Feriyanto, "Peran Fintech Dalam Meningkatkan Akses Keuangan Di Era Digital," *GEMILANG J. Manaj. dan Akunt.*, vol. 4, no. 3, pp. 99–114, 2024, doi: 10.56910/gemilang.v4i3.1573.
[33] C. Aliliele, I. S. Mbonu, and U. Iwuanyanwu, "A Review of API Governance and Risk Prioritization Frameworks in Modern Financial Institutions," pp. 395–433, 2023.

[34] A. Rajis, "A Conceptual Integration of Architecture, Project Management and Governance," *Int. J. Proj. Manag.*, vol. 8, no. 1, pp. 66–73, 2026, doi: 10.47672/ijpm.2926.