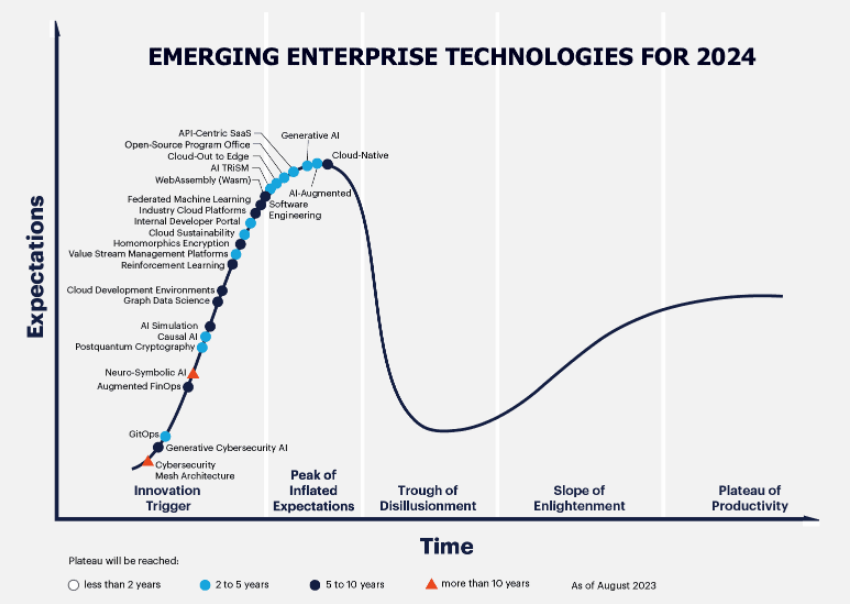
BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya teknologi digital di era sekarang, semakin banyak perusahaan yang ikut serta melakukan proses digitalisasi terhadap usahanya. Hal ini juga menjadi memicu terbentuknya teknologi baru untuk menompang proses bisnis tersebut, salah satunya dalam bidang *cloud computing* yang ditawarkan oleh berbagai *cloud service provider* seperti *Google Cloud Platform*, *Amazon Web Services*, *Micrsoft Azure*, dan masih banyak lagi. Konsep *cloud computing* berasal dari konsep arsitektur yang terdistribusi (*Distributed software architecture*) yang memiliki tujuan untuk memudahkan pengguna untuk memiliki *resource* yang tepat dan mudah di akses, khususnya dalam proses pengembangan perangkat lunak yang hadir dalam bentuk *cloud resources[1]*. *Cloud resources* merupakan sumber daya TI (*IT Resources*) yang dapat diakses melalui koneksi internet dengan cara berbayar melalui *cloud service provider* setiap kali dipergunakan [2].*Cloud computing* menjadi pilihan yang tepat untuk pelaku usaha dalam hal mengembangkan digitalisasi dengan menawarkan berbagai bentuk *cloud models* seperti IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*), CaaS (*Container as a Service*) maupun SaaS (*Software as a Service*)[1]. Hal ini dikarenakan sebagian dari kemampuan *cloud service* yang dapat mempermudah proses pengumpulan, pemrosesan, dan penyimpanan data secara daring melalui platform yang dimiliki oleh *cloud service provider[2]*.

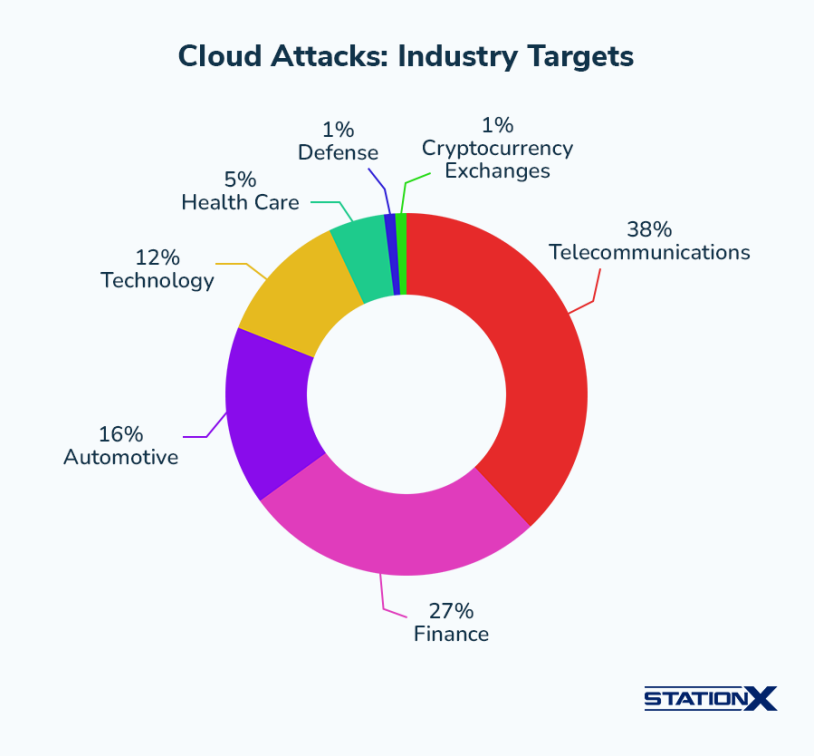


Gambar 1.1 : Prediksi Tren Teknologi yang digunakan Perushaan Tahun 2024

Sumber : Gartner IT *Syposium*, 2023, grafik oleh *US Cloud*

Dengan berkembang dan maraknya penggunaan *cloud computing* di era sekarang, tentu memiliki konsekuensi tersendiri terhadap serangan siber yang semakin marak. Hal tersebut juga disebabkan karena infrastruktur *cloud* mempergunakan protokol internet standar, juga menggunakan konsep *virtualization* [3]. *Virtualization* atau virtualisasi pada komputer merupakan proses penyediaan atau pembuatan perangkat keras, perangkat lunak, sistem operasi, sistem penyimpanan, atau sistem jaringan secara *virtual* dengan mengkedepankan skalabilitas dan kecepatan [4]. Keamanan merupakan bagian yang sangat penting dalam membangun *cloud architecture* yang baik, hal ini meliputi pengunaan *cloud resource* yang benar beserta konfigurasi *resource* tersebut agar sesuai dengan *security compliance* yang ada[1]. Terdapat beberapa usaha untuk meningkatkan postur keamanan yang dimiliki oleh *cloud service provider*, salah satunya adalah "*Autonomus Cloud Intrusion Response System* (ACIRS)" dan sebelumnya "*Network Intrusion Detection and Countermeasure Selection System* (NICE)", yang dimana teknologi *ACIRS* lebih baik dalam memitigasi resiko dalam

pengunaan *virtual network* yang dibuat dalam *cloud environment [1]*. Perkembangan teknologi *machine learning* juga menjadi batu loncatan dalam memperkuat keamanan yang ada, terutama penggunaannya dalam *cloud architecture*. Penggunaan *machine learning* dalam memperkuat keamanan *cloud resources*, berada pada kemampuannya untuk mendeteksi dan memberi peringatan kepada *system administrator* pada saat terjadinya serangan terhadap *cloud environment* yang ada, *machine learning* juga dapat dipergunakan untuk melakukan pengecekan dan penilaian terhadap *cloud infrastructure* yang ada [3].



Gambar 1.2 : Segmentasi Serangan Siber Melalui *Cloud Environment* Sektor Industrial

Sumber : *StationX*, 2024

Pilar keamanan merupakan salah satu hal yang menjadi prioritas dalam membuat arsitektur yang standar. Walaupun sudah ada standarisasi dan fitur- fitur yang menjadi penompang suatu sistem untuk memiliki keamanan yang baik, serangan terhadap sistem tetap dapat terjadi. Salah satu cara untuk meningkatkan

keamanan suatu sistem adalah dengan menerapkan *zero trust concept*. *Zero trust* merupakan paradigma dalam keamanan siber yang terfokus pada perlindungan terhadap *resources* yang ada dalam suatu sistem, konsep ini juga percaya akan akses yang diberikan kepada seseorang terhadap suatu sistem dapat berubah sesuai dengan kebutuhan yang ada dan hanya dibatas untuk kebutuhan tersebut saja [5]. Dengan menggunakan konsep ini, suatu sistem dapat ditingkatkan keamanannya tidak hanya dari ancaman eksternal, melainkan juga ancaman internal. Walaupun ancaman internal banyak disebabkan oleh kesalahan teknis, faktor *human error* merupakan faktor yang menyebabkan banyak ancaman keamanan pada suatu sistem [6]. Faktor tersebut menjadi salah satu penyumbang pelanggaran keamanan terbanyak, hal tersebut membuat manusia menjadi penghubung terlemah (*Weakest Link*) dalam keamanan siber [6]. Dengan menerapkan konsep *zero trust*, faktor-faktor yang menjadi penyebab dari pelanggaran keamanan dapat dieliminiasi satu-persatu. Faktor kesalahan manusia dapat ditanggulangi dengan menerapkan salah satu peraturan dalam konsep *zero trust* yaitu *princple of least privilege*. *Principle of least privilege* merupaan suatu konsep dimana semua akses yang diberikan kepada *user* eksternal maupun *user* internal dibatasi sesuai dengan keperluan masing-masing *user* atau akses granular [5]. Tidak hanya melindungi suatu sistem dari serangan internal saja, konsep ini juga mementingkan semua bagian yang bekerja dalam suatu infrastruktur sistem, konsep *zero trust* juga mementingkan keamanan semua komunikasi yang terjadi di dalam arsitektur sistem, polis atau peraturan terhadap suatu *resource* yang dinamis, dan observasi dan pemantauan kondisi integritas sistem yang rutin [5].

Gambar 1.3 : Potensi Ancaman Terhadap Keamanan *Cloud Data*

Sumber : *StationX*, 2024

Penerapan arsitektur *Zero Trust* dapat menyelesaikan berbagai permasalahan keamanan yang sering terjadi dalam lingkungan *cloud computing*, khususnya yang berkaitan dengan akses tidak sah dan kurangnya kontrol terhadap identitas pengguna. *Zero Trust Architecture* menerapkan prinsip "*never trust, always verify*", di mana setiap permintaan akses harus divalidasi berdasarkan identitas, konteks, dan kepatuhan terhadap kebijakan yang telah ditentukan. Pendekatan ini sangat relevan untuk menjawab tantangan keamanan modern yang kompleks dan dinamis, terutama dalam lingkungan *cloud* yang sangat terdistribusi. Berikut merupakan dua contoh studi kasus yang dapat diatasi melalui penerapan *Zero Trust Architecture*:

- *Unauthorized Access* di Waktu yang Tidak Tepat

  Seorang karyawan yang bertugas melakukan perubahan konfigurasi pada sistem database dijadwalkan untuk melakukannya pada malam hari. Namun karena ia telah memperoleh akses sejak siang hari, ia mencoba melakukan perubahan lebih awal guna mengantisipasi kendala saat eksekusi. Hal ini justru menyebabkan

downtime akibat kesalahan yang tidak disengaja. Dengan pendekatan *Zero Trust*, akses terhadap *resource* dapat dibatasi secara kontekstual, termasuk berdasarkan waktu, sehingga akses hanya aktif sesuai jadwal yang ditentukan. Kebijakan akses berbasis waktu (*time-limited access*) seperti ini dapat meminimalkan risiko gangguan operasional yang disebabkan oleh aktivitas di luar waktu yang diotorisasi.

- *Unaudited Access List* oleh Eks-Karyawan

  Dalam kasus lainnya, seorang mantan karyawan yang telah mengundurkan diri masih memiliki akses aktif terhadap cloud resource milik salah satu klien. Ia memanfaatkan akses tersebut untuk membuat *virtual machine* dan menjalankan aktivitas penambangan *cryptocurrency* secara ilegal. Hal ini menyebabkan konsumsi resource yang tidak sah dan berdampak pada kerugian finansial yang besar bagi perusahaan klien. Penerapan *Zero Trust* dapat mencegah insiden ini melalui automasi audit akses dan pemutusan hak akses berdasarkan perubahan status identitas pengguna. Selain itu, *Zero Trust* juga memungkinkan penerapan prinsip *least privilege* dan *monitoring* akses secara berkelanjutan guna mendeteksi serta memblokir aktivitas mencurigakan secara real-time.

Melihat kompleksitas dan risiko yang ditimbulkan dari kedua kasus tersebut, diperlukan pendekatan keamanan yang lebih adaptif dan presisi dalam memitigasi akses yang tidak sah serta penyalahgunaan hak akses di lingkungan *cloud*. *Zero Trust Architecture* menjadi pendekatan yang relevan karena mampu mengatur kontrol akses secara ketat berdasarkan identitas, waktu, dan konteks penggunaan. Penelitian ini bertujuan untuk menerapkan *Zero Trust Architecture* pada lingkungan *cloud computing* menggunakan *Microsoft Azure* sebagai upaya preventif terhadap potensi insiden keamanan, seperti *unauthorized access* dan *unaudited access list*. Melalui penerapan *Zero Trust*, diharapkan dapat tercipta

arsitektur keamanan cloud yang lebih tangguh, terukur, dan sesuai dengan kebutuhan keamanan sistem informasi modern.

1.2 Rumusan Masalah

Berdasarkan penjelasan yang telah diuraikan pada latar belakang, maka masalah yang akan diteliti dalam penelitian ini adalah: "Bagaimana cara mengimplementasikan konsep arsitektur *zero trust* pada *cloud environment* menggunakan *Microsoft Azure* sebagai *cloud provider* ?"

1.3 Tujuan Penelitian

Berdasarkan ruusan masalah yang ada, maka tujuan dari dilakukannya penelitian ini adalah: "Berhasil melakukan demonstrasi implementasi konsep *zero trust architecture* dalam *cloud environment* menggunakan *Microsoft Azure* sebagai *cloud provider*."

1.4 Manfaat Penelitian

Berikut merupakan manfaat yang ada dari dilakukannya penelitian ini:

1.4.1 Manfaat Bagi Praktisi

Informasi yang diperoleh dari hasil penelitian ini diharapkan dapat menjadi panduan bagi *cloud engineer* yang menggunakan *Microsoft Azure* sebagai *cloud provider* dalam menerapkan prinsip *Zero Trust Architecture* secara praktis. Selain itu, secara konseptual, hasil penelitian ini juga dapat dijadikan referensi oleh *cloud engineer* yang menggunakan penyedia layanan *cloud* lainnya, serta oleh praktisi yang ingin mulai mengimplementasikan pendekatan *Zero Trust* pada *cloud environment* yang sedang digunakan maupun yang akan dibangun. Meskipun pendekatan teknis yang digunakan dalam penelitian ini berfokus pada Azure, prinsip-

prinsip dasar *Zero Trust* yang diterapkan bersifat universal dan dapat diadaptasi sesuai dengan fitur dan layanan dari masing-masing *cloud provider*.

1.4.2 Manfaat Bagi Akademisi

Informasi yang diperoleh dari hasil penelitian ini dapat menjadi pedoman atau kerangka awal (*framework*) dalam mengimplementasikan konsep *Zero Trust Architecture* ke dalam suatu sistem, khususnya pada lingkungan *cloud*. Hasil penelitian ini juga memberikan pemahaman mendalam terkait konsep *Zero Trust Architecture*, *cloud computing*, serta potensi celah keamanan yang dapat ditemukan baik pada lingkungan *cloud* (*cloud environment*) maupun sistem lokal (*on-premises*). Selain itu, informasi yang dihimpun melalui penelitian ini dapat memperkaya literatur yang sudah ada serta menjadi data pendukung untuk penelitian selanjutnya yang mengangkat topik serupa dalam konteks keamanan sistem informasi dan arsitektur *cloud*.

1.5 Batasan Masalah

Batasan masalah yang akan diterapkan dalam penelitian ini adalah sebagai berikut:

1. Untuk mendapatkan tahapan implementasi yang lebih akurat, penulis hanya membatasi implementasi pada *cloud environment* yang terapat atau didukung oleh *Microsoft Azure* sebagai *cloud provider* yang digunakan.
2. Lingkup dari penelitian ini meliputi hal-hal berikut:
    - Mengetahui cara mengimplementasikan konsep *zero trust architecture* dalam *Microsoft Azure cloud environment*,
    - Mengetahui penggunaan *resources* pendukung dalam pembuatan *zero trust architecture*,
    - Melakukan pengaturan atas *resources* yang digunakan dalam menerapkan konsep *zero trust architecture*,

- Menghubungkan antara *user* dan *cloud resources* yang ingin diakses dengan berkaca terhadap konsep *zero trust*.

1.6 Sistematika Penelitian

Skripsi ini disusun dengan struktur sebagai berikut:

Bab 1 Pendahuluan

Dalam bab ini, akan dipaparkan tentang latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metodologi penelitian, dan sistematika penelitian.

Bab 2 Landasan Teori

Dalam bab ini akan dibahas literatur yang berisi tentang penjelasan terhadap teori pendukung, batasan konseptual, dan kerangka hipotesis yang bersumber dari penelitian, buku, dan literatur terdahulu yang akan digunakan dalam proses penelitian.

Bab 3 Metode Penelitian

Bab ini mencangkup metode dan teknik penelitian yang digunakan dalam proses penelitian yang akan dilakukan, meliputi rancangan penelitian, teknik implementasi, dan teknik analisis data.

Bab 4 Hasil Penelitian dan Pembahasan

Dalam bab ini akan dijelaskan hasil dan pembahasan dari analisi data terkait penelitian yang telah dilakukan.

Bab 5 Kesimpulan dan Saran

Bab ini mencangkup kesimpulan terhadap penelitan dan analisa yang telah dilakukan, keterbatasan penelitian, serta saran penulis yang berguna meningkatkan keamanan arsitektur sistem.