BAB 2

LANDASAN TEORI

2.1 Kajian Pustaka

Dalam melakukan dan menuliskan penelitian ini, penulis melakukan tinjauan pustaka terhadap penelitian- penelitian serupa maupun yang berhubungan dengan judul yang telah dilakukan oleh peneliti terdahulu. Hal ini dilakukan guna memperoleh informasi terkait kekurangan maupun kelebihan dari penelitian yang telah dilakukan sebelumnya. Penulis juga memperoleh teori yang akan digunakan dalam pembuatan landasan teori ilmiah pada skripsi ini.

Penelitian pertama yang ditinjau oleh penulis merupakan jurnal ilmiah yang ditulis oleh Sina Ahmadi pada tahun 2024. Dalam jurnal ini[7], dibahas tentang implementasi *Zero Trust Architecture* dalam *Cloud Network*, hal ini termasuk pengaplikasian, tantangan dalam implementasi, dan juga peluang pengembangan dalam pengaplikasiannya. Implementasi *zero trust architecture* (ZTA) dalam c*loud environment* akan memperkuat keamanan suatu arsitektur secara signifikan dibanding dengan penggunaan struktur keamanan tradisional, karena struktur yang digunakan dalam z*ero trust policy* memerlukan otentikasi lebih guna melindungi informasi yang bersifat sensitif dalam suatu sistem[7] . Jurnal ini juga implementasi ZTA di dalam arsitektur *cloud* seperti pemberian akses terhadap *user* untuk suatu *resource* yang ada di *cloud*, perlindungan akses jaringan yang digunakan dalam arsitektur *cloud*, serta segmentasi yang dapat dilakukan dalam penerapan ZTA. Seperti data yang telah disertakan oleh penulis pada bab sebelumnya, faktor internal menjadi penyumbang pelanggaran keamanan terbanyak dikarenakan manusia merupakan penghubung terlemah (*weakest link)* dalam suatu infrastruktur sistem. Model keamanan *zero trust* dapat mencegah terjadinya pelanggaran keamanan yang disebabkan oleh faktor internal karena ZTA sendiri menganggap tidak ada *user* yang dapat dipercaya, yang memungkinkan untuk melakukan pengecekan dan

pemantauan *user* yang berada di dalam sistem tersebut[7]. Setelah membahas tentang tantangan yang ada, diakhir jurnal ini juga dibahas tentang peluang implementasi ZTA pada arsitektur *cloud* kedepannya. Banyak peluang positif yang dapat digunakan dalam melakukan implementasi ZTA, hal ini dikarenakan seiring berkembangnya teknologi *cloud*, teknologi lain seperti *machine learning* (ML) dan *artificial intelligence* (AI) juga akan ikut berkembang dan dapat memperkuat deteksi ancaman yang ada secara *real-time[7]*. Kedepannya, ZTA akan mengintegrasikan sistem keamanan yang berfokus kepada *user* yang ada[7].

Penelitian kedua yang ditinjau oleh penulis merupakan artikel ilmiah yang ditulis oleh Himanshu Sharma pada tahun 2022. Dalam jurnal ini[8], dibahas tentang implementasi *Zero Trust Architecture* dalam *Cloud*, yang mengacu pada tujuannya untuk memperkuat sistem keamanan yang ada di dalam arsitektur *cloud*. Jurnal ini membantu memahami bagaimana evolusi model keamanan sistem yang ada, hingga akhirnya berkembang menjadi *Zero Trust Architecture* (ZTA). Sistem keamanan yang sekarang sering kali diterapkan merupakan hasil dari berkembangnya sistem keamanan terdahulu. Dalam artikel ini ditunjukkan bahwa perkembangan sistem keamanan komputer dimulai dari *perimeter-based security model*; Konsep keamanan ini mengacu pada penilaian ancaman yang ada pada sistem komputer lama, yang mana semua ancaman diyakini berasal dari faktor eksternal[8]. Paradigma dari ZTA adalah untuk memberikan akses terhadap suatu sistem dan memelihara akses tersebut agar terhindar dari ancaman yang ada[8]. Dalam menerapkan konsep ZTA di dalam suatu arsitektur *cloud*, diperlukan beberapa komponen utama yang akan mendukung sistem keamanan yang ada. Penggunaan *Identity and Access Management* (IAM) dengan mengharuskan setiap *user* memiliki *multi-factor authorization,* segmentasi jaringan dengan mengonfigurasi *virtual private network* yang ada dan menerapkan penggunaan VPN sebagai jembatan penghubung antara sistem *user* dengan sistem utama, dan mengintegrasi sistem dengan komponen *security information and system management* (SIEM) sebagai bentuk pemantauan sistem merupakan komponen utama yang perlu digunakan dalam mengimplementasikan ZTA terhadap suatu arsitektur *cloud*[8].

Kedua tinjauan pustaka yang dilakukan oleh penulis membahas tentang implementasi ZTA dalam suatu arsitektur *cloud*. Adapun perbedaan antara kedua tinjauan pustaka tersebut dengan penelitian yang akan dilakukan adalah keduanya hanya melakukan analisa terhadap implementasi ZTA yang dilakukan dalam arsitektur *cloud*, sedangkan penelitian ini bertujuan untuk melakukan pembuktian atas Implementasi ZTA yang dilakukan. Proses implementasi akan dilakukan dengan menggunakan *Microsoft Azure*, yang merupakan salah satu *cloud provider* yang ada. Dengan memahami kedua tinjauan pustaka di atas, penulis dapat mengetahui fondasi dan tantangan yang akan dihadapi dalam melakukan implementasi.

Tabel 2.1 Penelitian Terdahulu

No.	Nama Penulis	Tahun	Judul Penelitian	Rangkuman
1.	Sina Ahmadi	2024	Zero Trust Architecture in Cloud Networks: Application, Challenges, and Future Opportunities	• Memperkuat keamanan arsitektur cloud secara signifikan dibandingkan dengan struktur keamanan tradisional. • Memerhatikan akses yang diberikan kepada pengguna cloud secara detil dan dinamis. • Faktor internal sebagai penyumbang pelanggaran keamanan terbesar (manusia sebagai titik terlemah). • Peluang pengembangan ZTA dalam cloud ada

				pada perkembangan teknologi *Machine Learning* (ML) dan *Artifiial Intelligence* (AI) yang dapat mendukung deteksi ancaman secara *real-time*.
2.	Himanshu Sharma	2022	Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security	• ZTA muncul sebagai perkembangan lanjutan untuk mengatasi ancaman baik internal maupun eksternal. • Konsep ZTA memberikan dan memelihara akses ke sistem dengan memastikan perlindungan terhadap ancaman yang ada. • Membahas komponen-komponen utama dalam ZTA, yaitu *Identity Access Management* (IAM), segmentasi jaringan, dan integrasi *Security Information & Event Management* (SIEM).

2.2 Zero trust architecture

Zero trust architecture atau disingkat ZTA, merupakan salah satu kerangka (*framework*) berpikir yang menjadi standar dalam membuat suatu sistem yang aman. Kerangka ZTA sudah ada secara konseptual jauh sebelum maraknya penggunaan ZTA di kalangan sistem keamanan, konsep atau strategi ini disebut dengan "*Black Core*" (BCORE)[5]. Inti dari strategi ini adalah sistem keamanan yang ada pada suatu sistem akan terfokus kepada masing-masing transaksi (*transaction*) atau aksi (*action*/*event*) yang terjadi di dalam sistem tersebut. Secara definisi resmi menurut *National Institute of Standards and Technology* (NIST), ZTA adalah paradigma keamanan siber yang memiliki fokus terhadap proteksi setiap komponen dalam suatu sistem secara individu dan memiliki premis bahwa akses yang diberikan untuk masuk ke dalam sistem harus terus dievaluasi secara berkelanjutan[5].

Kerangka arsitektur ini terfokus terhadap setiap komponen yang ada di dalam sistem, meliputi semua komponen, koneksi antar komponen, dan semua *user* yang sedang ataupun dapat mengakses sistem tersebut secara lokal maupun *remote*. Konsep keamanan *zero trust* sendiri memberikan kumpulan konsep dan ide yang didesain untuk meminimalisir permukaan serangan yang dimiliki oleh suatu sistem, kerangka keamanan ZTA menggunakan konsep dan ide tersebut untuk membangun arsitektur dengan sistem keamanan yang mengedepankan hubungan antar komponen, perencanaan alur sistem, dan kebijakan akses dari sistem yang ada[5] .

2.2.1 Prinsip Zero trust architecture

Suatu infrastruktur yang akan menggunakan kerangka ZTA harus berpatokan pada prinsip-prinsip dasar berikut[5] :

- **Seluruh sumber data (*data sources*) dan layanan komputasi (*computing services*) akan dianggap sebagai komponen sistem**; Dalam suatu infrastruktur pastinya akan ada banyak segmentasi jaringan yang memiliki

komponen dan layanan masing-masing dengan skala yang beragam, dalam ZTA seluruh komponen dan sumber data yang keluar ataupun masuk ke dalam sistem akan dianggap sebagai komponen yang harus dilindungi.

- **Seluruh komunikasi yang terjadi antar komponen harus secara aman dimanapun lokasi komponen yang berkomunikasi *(secure line communication)*;** Dalam suatu infrastruktur *cloud*, komponen dapat tersebar tergantung dari lokasi dibuatnya komponen tersebut, dalam kerangka keamanan ZTA lokasi tersebut tidak akan dipertimbangkan tingkat keamanannya, maka yang akan diamankan adalah jalur komunikasi yang digunakan antara komponen-komponen tersebut.
- **Akses sistem yang ada akan diberikan dengan batasan waktu *(time-limited access)*;** Kerangka ZTA sangat ketat terhadap akses yang diberikan, terutama terhadap komponen yang akan mengakses titik-titik sensitif suatu sistem (panel admin, basis data, panel konfigurasi, dll.) yang dimana akan diberikan akses dengan adanya batasan waktu sesuai dengan penggunaan komponen yang ada dalam sistem.
- **Akses yang diberikan akan ditentukan oleh kebijakan yang dinamis *(dynamic access policy)*;** Akses yang diberikan akan bergantung keras terhadap kebijakan yang ada, dimana kebijakan tersebut harus tetap dinamis menyesuaikan dengan praktik terbaik dalam keamanan siber.
- **Komponen yang ada di dalam sistem harus selalu dipantau dan dievaluasi tingkat keamanannya secara berkala *(continuous system monitoring dan evaluation)*;** Komponen yang ada harus selalu dipantau baik dari segi kinerja maupun statusnya, tingkat keamanan yang ada juga harus dievaluasi secara berkala karena dalam kerangka ZTA tidak ada komponen yang dapat terus menerus dipercaya tingkat keamanannya.
- **Seluruh akses yang diberikan harus selalu dievaluasi secara dinamis sebelum diotorisasi *(evaluated access)*;** Akses yang diberikan terhadap suatu komponen atau *user* yang akan terhubung harus dievaluasi dengan jelas dan teliti sebelum melakukan otorisasi terhadap akses tersebut.

- **Informasi yang ada dalam komponen, jaringan, maupun akses yang diberikan harus selalu digunakan untuk analisa peningkatan postur keamanan *(system log analysis)*;** Informasi yang didapat dari setiap komponen, komunikasi antar jaringan, dan akses yang diberikan dapat berupa *logs* harus dikumpulkan dan digunakan untuk menganalisis potensi peningkatan maupun ancaman yang dapat digunakan untuk meningkatkan postur keamanan yang telah diterapkan, hal ini dilakukan agar postur keamanan tetap dinamis dan selalu diperbarui dengan praktik terbaik.

2.3 Cloud computing

Cloud computing merupakan salah satu tahap perkembangan teknologi informasi yang mengedepankan prinsip aksesibilitas *on-demand* pada layanan & produk komputasi. "*Cloud"-computing* merupakan teknologi infrastruktur siber yang menggabungkan teknologi terdahulu seperti *virtualization*, *distributed computing*, *networking,* dan *software services* ke dalam satu platform dengan aksesibilitas dan skalabilitas yang tinggi[9]. Dengan kelebihan tersebut, *cloud computing* menawarkan platform *on-demand* yang memiliki layanan dan produk komputasi yang beragam yang dapat digunakan sesuai dengan kebutuhan pengguna. Konsep yang mendukung *cloud computing* menjadi salah satu teknologi yang marak digunakan adalah komputasi melalui *service-oriented architecture* (SOA) yang merupakan layanan komputasi yang sudah diatur dan terintegrasi untuk pengguna yang dapat langsung dikonfigurasi dan digunakan[9]. Dengan SOA, pengguna dapat mengonfigurasi layanan komputasi dengan fungsi, spesifikasi, dan skala yang diinginkan yang dapat langsung digunakan[9].

Konsep *virtualization* adalah pilar yang cukup banyak menarik perhatian pengguna dalam menggunakan teknologi *cloud computing*. *Virtualization* adalah teknologi yang mengabstraksi dan mengisolasi fungsionalitas dasar dan perangkat keras dari suatu sistem, hal ini memungkinkan portabilitas dari fungsi-fungsi yang lebih tinggi dengan membagi/ mengagregasi perangkat lunak yang digunakan[9]. Secara lebih sederhananya, *virtualization* adalah pembuatan perangkat keras,

perangkat lunak, platform, perangkat penyimpanan, sistem operasi, maupun perangkat jaringan secara virtual (tidak asli) yang secara skala, funsional, maupun spesifikasinya dapat dirubah dengan cepat[4].

2.3.1 Model layanan dalam *Cloud computing*

Dalam *cloud computing*, layanan seperti perangkat lunak, infrastruktur perangkat keras, infrastruktur jaringan, hingga perangkat penyimpanan akan disediakan untuk pengguna, *cloud computing* memiliki 3 model layanan:

1. ***Private Cloud***

   Private cloud merupakan model layanan *cloud computing* yang lingkupnya hanya digunakan oleh organisasi tertentu yang dimana semua layanan yang digunakan hanya dapat diakses oleh sejumlah orang[4].

2. ***Public Cloud***

   Public cloud merupakan model layanan *cloud computing* yang dapat diakses secara publik dengan koneksi internet, akses publik ini diperuntukkan kepada pengguna yang ingin menggunakan layanan *cloud computing* secara personal dengan basis pembayaran *pay-per use[4]*.

3. ***Hybrid Cloud***

   Hybrid Cloud merupakan gabungan antara kedua model sebelumnya dan menawarkan kelebihan dari masing-masing model. Layanan *hybrid cloud* memungkinkan organisasi untuk menggunakan layanan *cloud computing* secara privat dalam lingkup internalnya dan juga publik dalam lingkup eksternalnya (*public-facing services*)[10].

2.4 Microsoft Azure

Dalam menggunakan layanan *cloud computing*, pengguna harus mengakses layanan yang ditawarkan melalui penyedia layanan (*cloud service providers*) yang beragam. Penyedia layanan *cloud service* merupakan model bisnis teknologi informasi yang menyediakan layanan *cloud computing* yang dapat diakses melalui internet[2]. Layanan yang ditawarkan biasanya memiliki berbagai bentuk, mulai dari *Infrastructure as a Service* (IAAS), *Platform as a Service* (PAAS), *Software as a Service* (SAAS), hingga yang paling baru *Infrastructure as a Code* (IAAC).

Sebagai penyedia layanan *cloud computing*, perusahaan yang bergerak dibidang ini menyediakan layanan dengan skalabilitas tinggi, yang dapat diakses secara *on-demand* melalui jaringan internet, meliputi *cloud-based computing*, penyimpanan data, platform, hingga aplikasi-aplikasi pendukung bagi pelaku bisnis, organisasi, hingga penggunaan personal[2]. Salah satu penyedia layanan ini adalah *Azure* yang dikelola oleh *Microsoft*. *Microsoft Azure* merupakan produk dari *Microsoft* yang masih terus berkembang dan memiliki cakupan layanan yang luas untuk keperluan penggunaan layanan *cloud computing[11] . Microsoft Azure* sendiri menawarkan layanan *cloud* dengan tingkat *availability* yang tinggi, integrasi antara *private* dan *public cloud*, integrasi sistem keamanan *cloud* dengan *Microsoft Defender for Cloud*, hingga integrasi dengan produk & perangkat lunak dari *Microsoft[12]*. Penggunaan *Microsoft Azure* dalam penelitian ini akan menujukan implementasi ZTA yang dapat dilakukan dengan memanfaatkan layanan keamanan yang ditawarkan oleh *Micrososft Azure*, implementasi juga akan dilakukan dengan menggunakan model *hybrid cloud* yang dapat digunakan dengan menggunakan *Microsoft Azure*. Selain itu, pemilihan *Microsoft Azure* sebagai media penelitian disebabkan karena *Microsoft Azure* merupakan salah satu dari 3 penyedia layanan *cloud* yang terdiri atas *Microsoft Azure, Amazon Web Services* (AWS), dan *Google Cloud Platform* (GCP) [2].