ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

PENDEKATAN FILSAFAT ILMU PADA CLOUD SECURITY

Jamaluddin✉, Muhammad Zarlis, Zulkifli Nasution, Syahril Efendi
Fasilkom-TI, Universitas Sumatera Utara, Medan, Indonesia
Email: jac.satuno@gmail.com

DOI: https://doi.org/10.46880/jmika.Vol5No2.pp162-168

ABSTRACT

Scientific developments have given birth to new branches of science, one of which is the field of computer science which is one branch of science that has a fast development. So, the philosophy of computer science is a deep thought to obtain the truth, meaning, and purpose of the values of computer science for human life. The development of computing continues to the stage of cloud computing, which originally came from the time-sharing and multitasking features found in each operating system. A security risk that companies considering migrating to the cloud should not ignore is that posed by sharing vendor resources with other cloud users. Security controls in cloud computing are like security controls in any IT environment. The important concept in this regard is that while the company loses a significant amount of control over its resources, services, and applications, it must keep its security and privacy policies accountable. The application of the philosophy of science in security systems, especially in cloud storage security systems is something that must be done as a review of previous studies.
Keyword: Philosophy, Cloud Computing, Security.

ABSTRAK

Perkembangan keilmuan telah melahirkan cabang-cabang ilmu baru, satu diantaranya adalah bidang ilmu komputer yang merupakan salah sati cabang keilmuan yang memiliki perkembangan yang cukup cepat. Jadi filsafat ilmu komputer adalah pemikiran yang sedalam-dalamnya untuk memperoleh kebenaran, makna dan tujuan akan nilai-nilai ilmu komputer bagi kehidupan manusia. Perkembangan komputasi terus berlanjut hingga ke tahapan komputasi awan (*cloud computing),* yang mana pada awal mulanya berasal dari fitur *time sharing* dan *multitasking* yang terdapat pada setiap sistem operasi. Risiko keamanan yang tidak boleh diabaikan oleh perusahaan yang mempertimbangkan migrasi ke *cloud* adalah yang ditimbulkan oleh berbagi sumber daya vendor dengan pengguna *cloud* lainnya. Kontrol keamanan dalam komputasi awan mirip dengan kontrol keamanan di lingkungan TI mana pun. Konsep penting dalam hal ini adalah bahwa sementara perusahaan kehilangan sejumlah besar kendali atas sumber daya, layanan, dan aplikasi, ia harus menjaga akuntabilitas kebijakan keamanan dan privasi. Penerapan filsafat ilmu dalam sistem keamanan, khususnya pada sistem keamanan *cloud storage* merupakan hal yang harus dilakukan sebagai penelaahan dari kajian-kajian yang telah dilakukan sebelumnya.
Kata Kunci: Filsafat, Komputasi Awan, Keamanan.

PENDAHULUAN

Inti dari filsafat adalah berpikir, dan berpikir adalah sebuah tindakan manusia yang berfifat eksistensial, utuh dan menyeluruh. Meskipun demikian, usaha mendekati arti filsafat secara filosofis, bukan sekedar mengandaikan sebuah pengertian yang bersifat langsung dan lurus. Berbagai latar perbedaan pemikiran filosofis tentang arti filsafat, pada akhirnya mengandung berbagai kebenaran dalam pengembangan pemikiran. Kebenaran ilmu-ilmu empiris, seperti biologi, fisika dan geografi memiliki kedudukan yang sama dengan kebenaran ilmu-ilmu normative seperti ilmu hukum dan etika.

Perkembangan keilmuan telah melahirkan cabang-cabang ilmu baru, satu diantaranya adalah bidang ilmu komputer yang merupakan salah sati cabang keilmuan yang memiliki perkembangan yang cukup cepat. Ilmu komputer merupakan ilmu pengetahuan yang pengujian kebenarannya dilakukan melalui metode ilmiah yang menggunakan objek komputer digital. Penerapan filsafat pada bidang ilmu komputer bisa diartikan bahwa filsafat merupakan kebenaran pemikiran yang telah diuji. Jadi filsafat ilmu komputer adalah pemikiran yang sedalam-dalamnya untuk memperoleh kebenaran, makna dan tujuan akan nilai-nilai ilmu komputer bagi kehidupan manusia.

Perkembangan komputasi terus berlanjut hingga ke tahapan komputasi awan (*cloud computing),* yang mana pada awal mulanya berasal dari fitur *time sharing* dan *multitasking* yang terdapat pada setiap sistem

operasi. Fitur inilah yang menjadi pijakan dalam mengembangkan komputasi awan.

Cloud computing adalah inovasi pada bidang teknologi informatika yang dapat dimanfaatkan untuk membantu pekerjaan manusia. Pada saat sekarang ini sudah banyak aplikasi berbasis *cloud computing* yang dapat kita manfaatkan pada kehidupan sehari-hari misalnya aplikasi media sosial seperti *facebook*, twitter, *instagram*, tiktok dan lain sebagainya. Selain media sosial, terdapat juga *platform cloud computing* yang dapat dimanfaatkan secara gratis seperti fasilitas untuk membuat *website, blog* bahkan *platform* untuk pembelajaran daring seperti *Google Classroom, Edmodo*, *Cisco Webex* dan lain sebagainya. Selain penggunaan pada individu, terdapat juga *platform cloud computing* yang disediakan untuk kebutuhan bisnis dan pemerintahan. Penggunaan *platform cloud computing* memberikan kemudahan bagi pengguna, khususnya bagi perusahaan untuk memanfaatkan teknologi cloud ini tanpa harus menyiapkan infrastruktur hardware, software maupun aplikasi yang digunakan terlebih dahulu. Pemanfaatan *platform cloud computing* dapat menutunkan biaya produksi bagi perusahaan, karena tidak perlu lagi menyediakan infrastruktur yang diperlukan.

Salah satu fasilitas *cloud* yang disediakan oleh penyedia layanan *cloud* adalah *cloud storage. Cloud storage* merupakan layanan penyimpanan data ataupun informasi dari pengguna pada media penyimpanan yang berbasis internet. *Cloud Storage* sekarang ini sudah menjadi sebuah hal yang umum digunakan baik oleh individu maupun oleh perusahaan dalam penyimpanan data. Salah satu kelebihan dari *cloud storage* adalah kemudahan dalam akses data yang dapat dilakukan dari manapun dan kapanpun asalkan piranti yang kita gunakan terkoneksi dengan internet. Selain itu, *cloud storage* juga memudahkan dalam penyimpanan data dibandingkan dengan media penyimpanan data tradisional seperti *flashdisk* ataupun *hardisk eksternal*. Media penyimpanan pada *cloud storage* ada yang gratis dan ada yang berbayar. Kita dapat menggunakan beberapa *flatform cloud storage* gratis yang disediakan oleh penyedia layanan seperti *Google Drive, Dropbox* dan lain sebagainya.

Layanan *cloud storage* memiliki beberapa keunggulan diantaranya keamanan data, privasi, kemudahan dalam pengelolaan dan pengaksesan data, *real-time sync*, fasilitas pencadangan (*back-up*) yang mudah dan *collaboration tools* serta fasilitas lainnya (Cloudraya, 2020). Salah satu fasilitas layanan yang sering menjadi permasalahan adalah sisi keamanan data. Penggunaan *cloud storage* dalam penyimpanan data yang kita lakukkan memungkinkan penyedia layanan untuk menyimpan data tersebut pada *server* yang berlokasi pada pusat data penyedia layanan *cloud storage* tersebut.

Sistem keamanan *cloud storage* sebenarnya sudah baik, dimana data yang kita simpan pada layanan *cloud storage* tersebut hanya dapat diakses oleh pemilik data. Bahkan penyedia layanan *cloud storage* juga tidak dapat mengakses data jika tidak pemilik data tidak memberikan izin akses terhadap data tersebut. Tapi sistem keamanan yang diterapkan oleh penyedia layanan *cloud storage* terkadang dapat ditembus oleh pihak lain. Kebocoran data yang baru-baru ini terjadi pada salah satu layanan sosial media yang popular, dimana terdapat 533 juta data pengguna yang bocor, termasuk 130 ribu pengguna yang berasal dari Indonesia (Riyanto, 2021). Munculnya permasalahan keamanan data pada layanan *cloud storage* yang sering terjadi pada pengguna layanan *cloud storage* mendasari penulis untuk membangun sebuah model keamanan data yang dapat digunakan oleh pengguna layanan *cloud storage* dalam penyimpanan data pribadinya.

Pada artikel ini penulis membahas tentang pendekatan filsafat ilmu pada bidang keamanan sistem, khususnya pada keamanan *cloud computing.*

KAJIAN LITERATUR

Filsafat Ilmu

Filsafat merupakan dasar dari segala ilmu pengetahuan. Filsafat merupakan konsep pemikiran yang universal, menyeluruh dan mendasar (Ginting & Situmorang, 2008). Filsafat ilmu adalah salah satu cabang ilmu filsafat yang secara khusus meletakkan ilmu sebagai objek material. Filsafat dan Ilmu merupakan dua kata yang sangat saling berkaitan baik secara substansial maupun historis. Lahirnya suatu ilmu tidak dapat dipisahkan dari peranan filsafat, sedangkan perkembangan ilmu memperkuat keberadaan filsafat. Hal ini berlaku bagi semua ilmu yang terdapat di seluruh pelosok dunia ini, termasuk ilmu komputer yang didalamnnya juga sangat berkembang beberapa cabang ilmu seperti data mining, machine learning, jaringan komputer, rekayasa perangkat lunak dan masih banyak lagi yang lainnya (Fachruddin, 2016).

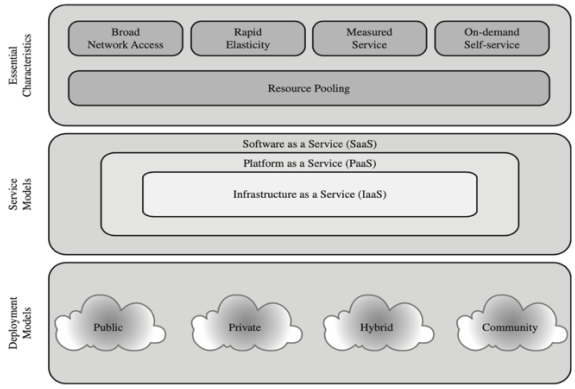
Filsafat Ilmu Komputer

Ilmu Komputer adalah bidang ilmu yang membahas mengenai pemrosesan informasi dengan struktur informasi dan prosedur yang masuk ke dalam representasi dari pemrosesan tersebut, dan dengan implementasinya dalam sistem pemrosesan informasi

(Colburn, 2013). Ilmu komputer merupakan ilmu pengetahuan yaitu pengetahuan yang telah diuji kebenarannya melalui metode ilmiah yang objeknya adalah komputer digital dan fenomena di sekitar mereka (sebagai pemroses dan penyaluran informasi) (Colburn, 2013). Filsafat komputer bisa diartikan bahwa filsafat adalah hasil pemikiran yang sedalam-dalamnya dimana kebenaranya telah diuji kemudian hasil itu menjadi ilmu pengetahuan untuk umum. Dalam hal ini yaitu ilmu pengetahuan tentang komputer yang tujuannya mempelajari nilai-nilai yang mempunyai manfaat yang terkandung dalam komputer. Jadi filsafat ilmu komputer adalah pemikiran yang sedalam-dalamnya untuk memperoleh kebenaran, makna, tujuan serta nilai-nilai ilmu komputer bagi kehidupan manusia.

Cloud Computing

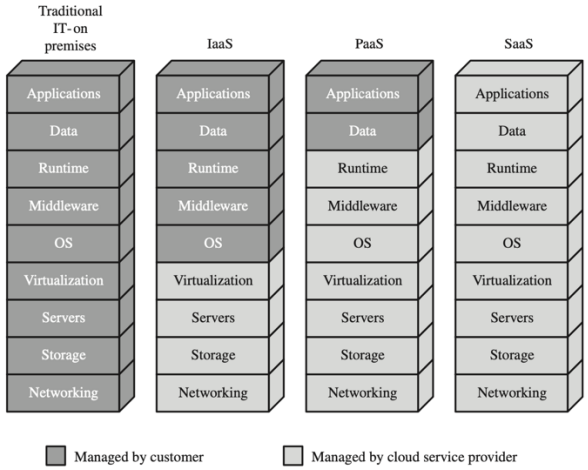
Sekarang ini terdapat tren baru yang semakin menonjol di banyak organisasi ataupun untuk memindahkan sebagian besar atau bahkan semua operasi teknologi informasi (TI) ke infrastruktur yang terhubung ke internet yang dikenal sebagai *cloud computing*. NIST mendefinisikan *cloud computing* seperti yang ditampilkan pada gambar berikut:



Sumber: (Mell & Grance, 2011)

Gambar 1. Elemen-Elemen *Cloud Computing*

Model dan karakteristik yang diilustrasikan pada gambar 1 diatas merupakan karakteristik yang penting pada *cloud computing*, yang meliputi *broad network access, rapid elasticity, measured service, on-demand self-service,* dan *resource pooling.* NIST SP 800-145 mendefinisikan tiga model layanan yang dijadikan alternatif layanan *cloud computing* yakni *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS) (Mell & Grance, 2011). SaaS memberikan layanan kepada pengguna dalam bentuk perangkat lunak (*software),* khususnya *software* aplikasi yang dapat diakses secara langsung dari *cloud.* SaaS memungkinkan pengguna untuk menggunakan aplikasi yang berjalan pada infrastruktur penyedia layanan. Aplikasi dapat diakses oleh pengguna melalui *interface* sederhana seperti pada *web browser*. Contoh layanan SaaS adalah Google Gmail, Microsoft 365, Citrix GoToMeeting, dan Cisco WebEx. PaaS menyediakan layanan kepada pengguna dalam bentuk platform sebagai lokasi aplikasi dijalankan, dimana PaaS menyediakan platform software yang berguna, ditambah sejumlah pengembangan seperti Bahasa pemrograman, lingkungan run-time, dan alat lain yang membantu dalam menyebarkan aplikasi baru. Sehingga dapat kita katakana bahwa PaaS adalah sistem operasi di cloud. Sedangkan pada layanan IaaS, pengguna memiliki akses ke sumber daya infrastruktur cloud. Pengguna layanna IaaS tidak mengelola atau mengontrol sumber daya infratruktur cloud tetapi memiliki control akan sistem operasi, aplikasi yang diterapkan dan kemungkinan control terbatas pada komponen jaringan tertentu (misalnya firewall host)



Sumber: (Stallings & Brown, 2018)

Gambar 2. Model Layanan Cloud

METODOLOGI

Penulisan artikel penelitian ini penulis menggunakan metode studi literatur yang merupakan cara untuk menyelesaikan permasalahan dengan menelusuri sumber-sumber tulisan yang pernah dipublikasikan sebelumnya (Sugiyono, 2013). Adapun sumber tulisan yang digunakan oleh penulis adalah buku, artikel pada jurnal ilmiah dan hasil penelitian lainnya.

PEMBAHASAN

Konsep Cloud Security

Penggunaan komputasi awan menimbulkan sejumlah masalah keamanan, khususnya di bidang keamanan. Keamanan penting untuk berbagai infrastruktur termasuk pada infrastruktur komputasi

perusahaan. Perusahaan berusaha keras untuk mengamankan sistem komputasi lokal, sehingga tidak mengherankan bahwa keamanan menjadi pertimbangan utama saat menambah atau mengganti sistem lokal dengan layanan komputasi awan. Menghilangkan masalah keamanan sering menjadi prasyarat untuk diskusi lebih lanjut tentang memigrasikan sebagian atau seluruh arsitektur komputasi organisasi ke layanan komputasi awan (*cloud*).

Risiko keamanan yang tidak boleh diabaikan oleh perusahaan yang mempertimbangkan migrasi ke *cloud* adalah yang ditimbulkan oleh berbagi sumber daya vendor dengan pengguna *cloud* lainnya. Penyedia *cloud* harus waspada terhadap pencurian atau serangan penolakan layanan oleh penggunanya dan pengguna harus dilindungi satu sama lain. Virtualisasi dapat menjadi mekanisme yang kuat untuk mengatasi potensi risiko ini karena melindungi dari sebagian besar upaya pengguna untuk menyerang satu sama lain atau infrastruktur penyedia. Namun, tidak semua sumber daya divirtualisasikan, dan tidak semua lingkungan virtualisasi bebas bug. Virtualisasi yang salah dapat memungkinkan kode pengguna untuk mengakses bagian sensitif dari infrastruktur penyedia atau sumber daya pengguna lain. Sekali lagi, masalah keamanan ini tidak unik untuk cloud dan serupa dengan yang terlibat dalam pengelolaan pusat data non-cloud, di mana aplikasi yang berbeda perlu dilindungi satu sama lain.

Masalah keamanan lain yang harus dipertimbangkan oleh bisnis adalah sejauh mana pelanggan dilindungi terhadap penyedia, terutama di bidang kehilangan data yang tidak disengaja. Misalnya, dalam hal peningkatan infrastruktur penyedia, apa yang terjadi pada perangkat keras yang dihentikan atau diganti? Sangat mudah untuk membayangkan sebuah hard disk dibuang tanpa benar-benar dibersihkan dari data pelanggan. Juga mudah untuk membayangkan bug atau kesalahan perizinan yang membuat data pelanggan terlihat oleh pengguna yang tidak berwenang. Enkripsi tingkat pengguna mungkin merupakan mekanisme bantuan mandiri yang penting bagi pelanggan, tetapi bisnis harus memastikan bahwa perlindungan lain tersedia untuk menghindari kehilangan data yang tidak disengaja.

Karena semakin banyak bisnis memasukkan layanan cloud ke dalam infrastruktur jaringan perusahaan mereka, keamanan komputasi awan akan tetap menjadi isu penting. Contoh kegagalan keamanan komputasi awan berpotensi memiliki efek mengerikan pada minat bisnis dalam layanan cloud. Ini menginspirasi penyedia layanan untuk serius dalam menggabungkan mekanisme keamanan yang akan menghilangkan kekhawatiran pelanggan potensial. Beberapa penyedia layanan telah memindahkan operasi mereka ke pusat data Tingkat 4 untuk mengatasi kekhawatiran pengguna tentang ketersediaan dan redundansi. Karena begitu banyak bisnis tetap enggan untuk merangkul komputasi awan secara besar-besaran, penyedia layanan awan harus terus bekerja keras untuk meyakinkan calon pelanggan bahwa dukungan komputasi untuk proses bisnis inti dan aplikasi penting misi dapat dipindahkan dengan aman dan aman ke awan.

Pendekatan Cloud Security

Secara umum, kontrol keamanan dalam komputasi awan mirip dengan kontrol keamanan di lingkungan TI mana pun. Namun, karena model operasional dan teknologi yang digunakan untuk mengaktifkan layanan cloud, komputasi awan dapat menimbulkan risiko yang spesifik untuk lingkungan cloud. Konsep penting dalam hal ini adalah bahwa sementara perusahaan kehilangan sejumlah besar kendali atas sumber daya, layanan, dan aplikasi, ia harus menjaga akuntabilitas kebijakan keamanan dan privasi.

Aliansi Keamanan Cloud [CSA13] mencantumkan hal berikut sebagai ancaman keamanan khusus cloud teratas:

1. Penyalahgunaan dan penggunaan *cloud computing*.
2. Antarmuka dan API's yang tidak aman.
3. *Malicious insiders*.
4. Permasalahan *shared technology*.
5. Kehilangan atau kebocoran data.
6. Pembajakan akun atau layanan.
7. *Unknown risk profile*.

Ada banyak cara untuk mengkompromikan data. Penghapusan atau perubahan catatan tanpa cadangan konten asli adalah contoh yang jelas. Membatalkan tautan rekaman dari konteks yang lebih besar dapat membuatnya tidak dapat dipulihkan, seperti halnya penyimpanan pada media yang tidak dapat diandalkan. Kehilangan kunci penyandian dapat mengakibatkan kehancuran yang efektif. Akhirnya, pihak yang tidak berwenang harus dicegah untuk mendapatkan akses ke data sensitif.

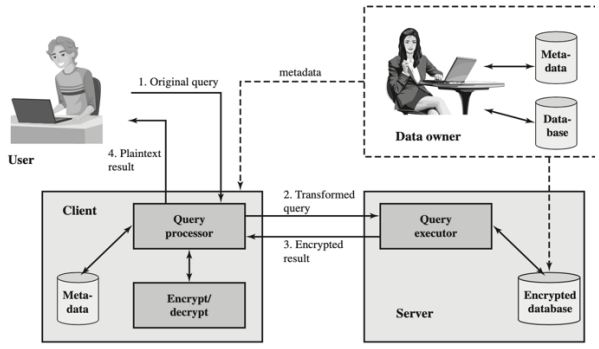
Ancaman kompromi data meningkat di cloud, karena jumlah, dan interaksi antara, risiko dan tantangan yang unik untuk cloud atau lebih berbahaya karena karakteristik arsitektur atau operasional lingkungan cloud.

Lingkungan basis data yang digunakan dalam komputasi awan dapat sangat bervariasi. Beberapa

penyedia mendukung model multi-instans, yang menyediakan DBMS unik yang berjalan pada instans VM untuk setiap pelanggan cloud. Ini memberi pelanggan kendali penuh atas definisi peran, otorisasi pengguna, dan tugas administratif lainnya yang terkait dengan keamanan. Penyedia lain mendukung model multi-penyewa, yang menyediakan lingkungan yang telah ditentukan sebelumnya untuk pelanggan cloud yang dibagikan dengan penyewa lain, biasanya melalui penandaan data dengan pengidentifikasi pelanggan. Pemberian tag memberikan tampilan penggunaan eksklusif instans, tetapi bergantung pada penyedia cloud untuk membangun dan memelihara lingkungan database yang aman.

Data harus diamankan saat diam, dalam perjalanan, dan digunakan, dan akses ke data harus dikontrol. Klien dapat menggunakan enkripsi untuk melindungi data dalam perjalanan, meskipun ini melibatkan tanggung jawab manajemen utama untuk CSP. Klien dapat menerapkan teknik kontrol akses, tetapi, sekali lagi, CSP terlibat sampai batas tertentu tergantung pada model layanan yang digunakan.

Untuk data saat istirahat, ukuran keamanan yang ideal adalah klien mengenkripsi database dan hanya menyimpan data terenkripsi di cloud, dengan CSP tidak memiliki akses ke kunci enkripsi. Selama kunci tetap aman, CSP tidak memiliki kemampuan untuk menguraikan data, meskipun korupsi dan serangan penolakan layanan lainnya tetap menjadi risiko. Model yang digambarkan pada Gambar 3 bekerja sama baiknya ketika data disimpan di awan.



Sumber : (Stallings & Brown, 2018)

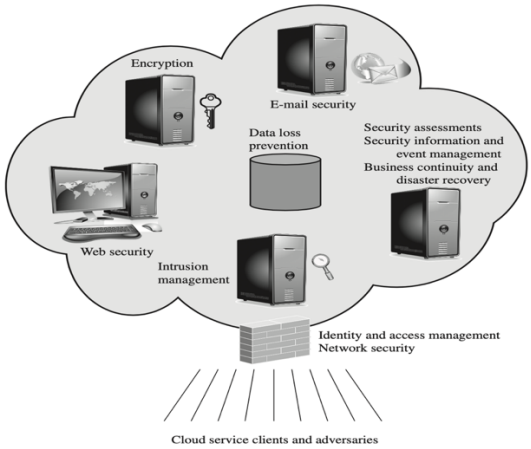
Gambar 3. Skema Enkripsi Basis Data

Di luar perlindungan dan isolasi data, penyedia layanan cloud (CSP) perlu mengatasi pertimbangan keamanan yang lebih luas untuk perlindungan asetnya. Gambar 4a, diadaptasi dari [ENIS15], menyarankan kategorisasi aset ini untuk tiga model layanan cloud. Dua lapisan terbawah yang ditunjukkan pada gambar termasuk organisasi dan fasilitas. Organisasi menunjukkan sumber daya manusia dan kebijakan serta prosedur untuk memelihara fasilitas dan mendukung penyampaian layanan. Fasilitas menunjukkan struktur fisik dan pasokan seperti jaringan, pendingin, dan catu daya. Di atas tingkat ini adalah aset khusus untuk penyediaan layanan. Untuk IaaS, CSP memelihara hypervisor dan/atau OS di setiap servernya, serta perangkat lunak jaringan untuk interkoneksi server CSP dan koneksi ke konsumen layanan cloud (CSC). Ditambahkan ke aset ini untuk PaaS adalah perpustakaan, middleware, dan perangkat lunak lain untuk mendukung aplikasi CSC. Untuk SaaS, CSP juga memiliki aset perangkat lunak aplikasi untuk penggunaan CSC.

Istilah Security as a Service (SaaS) umumnya berarti paket layanan keamanan yang ditawarkan oleh penyedia layanan yang mengalihkan sebagian besar tanggung jawab keamanan dari perusahaan ke penyedia layanan keamanan. Di antara layanan yang biasanya disediakan adalah otentikasi, anti-virus, antimalware/spyware, deteksi intrusi, dan manajemen peristiwa keamanan. Dalam konteks komputasi awan, keamanan awan sebagai layanan, yang disebut SecaaS, adalah segmen dari penawaran SaaS dari CSP. Gambar 4b menunjukkan tugas keamanan utama yang menjadi tanggung jawab CSP dan CSC. Tingkat terendah dari diagram berkaitan dengan masalah organisasi yang berkaitan dengan pengelolaan persediaan dan fasilitasnya. Tingkat berikutnya dari Gambar 4b mencakup keamanan fisik fasilitas. Di atas itu, tergantung pada model layanan, CSP bertanggung jawab untuk keamanan berbagai kemampuan perangkat lunak.

CSA mendefinisikan SecaaS sebagai penyediaan aplikasi dan layanan keamanan melalui cloud baik ke infrastruktur dan perangkat lunak berbasis cloud, atau dari cloud ke sistem on-premise pelanggan [CSA11]. CSA telah mengidentifikasi kategori layanan SecaaS berikut:

1. Manajemen identitas dan akses.
2. Pencegahan kehilangan data
3. Keamanan web
4. Keamanan e-mail
5. Penilaian keamanan
6. Manajemen intrusi
7. Informasi keamanan dan manajemen kegiatan
8. Enkripsi
9. Kesinambungan bisnis dan pemulihan bencana
10. Keamanan Jaringan



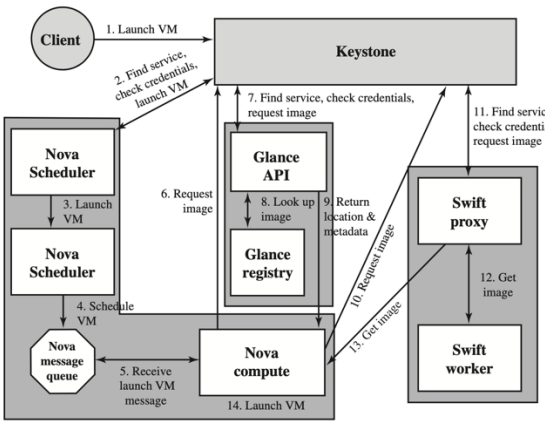
Sumber: (Stallings & Brown, 2018)

Gambar 4. Elemen dari Layanan Cloud SaaS

OpenStack adalah proyek perangkat lunak open-source dari OpenStack Foundation yang bertujuan untuk menghasilkan sistem operasi cloud open-source [ROSA14, SEFR12]. Tujuan utamanya adalah untuk memungkinkan pembuatan dan pengelolaan kelompok besar server pribadi virtual di lingkungan komputasi awan. OpenStack tertanam, sampai tingkat tertentu, ke dalam infrastruktur pusat data dan produk komputasi awan yang ditawarkan oleh Cisco, IBM, Hewlett-Packard, dan vendor lainnya. Ini menyediakan IaaS multi-penyewa, dan bertujuan untuk memenuhi kebutuhan awan publik dan pribadi terlepas dari ukurannya, dengan menjadi sederhana untuk diterapkan dan dapat diskalakan secara besar-besaran.

OpenStack OS terdiri dari sejumlah modul independen, yang masing-masing memiliki nama proyek dan nama fungsional. Struktur modular mudah ditingkatkan dan menyediakan serangkaian layanan inti yang umum digunakan. Biasanya, komponen dikonfigurasi bersama untuk menyediakan kemampuan IaaS yang komprehensif. Namun, desain modular sedemikian rupa sehingga komponen umumnya mampu digunakan secara mandiri.

Modul keamanan untuk OpenStack adalah Keystone. Keystone menyediakan layanan keamanan bersama yang penting untuk infrastruktur komputasi awan yang berfungsi. Gambar 5 mengilustrasikan cara Keystone berinteraksi dengan komponen Open-Stack lainnya untuk meluncurkan VM baru. Nova adalah modul perangkat lunak manajemen yang mengontrol VM dalam platform komputasi awan IaaS. Ini mengelola siklus hidup instance komputasi di lingkungan OpenStack. Tanggung jawab mencakup pemijahan, penjadwalan, dan penghentian mesin sesuai permintaan. Dengan demikian, Nova memungkinkan perusahaan dan penyedia layanan untuk menawarkan sumber daya komputasi sesuai permintaan dengan menyediakan dan mengelola jaringan VM yang besar. Glance adalah sistem pencarian dan pengambilan gambar disk VM. Ini menyediakan layanan untuk menemukan, mendaftar, dan mengambil gambar virtual melalui API. Swift adalah penyimpanan objek terdistribusi yang menciptakan ruang penyimpanan yang redundan dan dapat diskalakan hingga beberapa petabyte data. Penyimpanan objek tidak menyajikan sistem file tradisional, melainkan sistem penyimpanan terdistribusi untuk data statis seperti gambar VM, penyimpanan foto, penyimpanan email, cadangan, dan arsip.



Gambar 5. Virtual Machine in OpenStack

KESIMPULAN

Risiko keamanan yang tidak boleh diabaikan oleh perusahaan yang mempertimbangkan migrasi ke *cloud* adalah yang ditimbulkan oleh berbagi sumber daya vendor dengan pengguna *cloud* lainnya. Penyedia *cloud* harus waspada terhadap pencurian atau serangan penolakan layanan oleh penggunanya dan pengguna harus dilindungi satu sama lain. Kontrol keamanan dalam komputasi awan mirip dengan kontrol keamanan di lingkungan TI mana pun. Namun, karena model operasional dan teknologi yang digunakan untuk mengaktifkan layanan cloud, komputasi awan dapat menimbulkan risiko yang spesifik untuk lingkungan cloud. Konsep penting dalam hal ini adalah bahwa sementara perusahaan kehilangan sejumlah besar kendali atas sumber daya, layanan, dan aplikasi, ia harus menjaga akuntabilitas kebijakan keamanan dan privasi.

Penerapan filsafat ilmu dalam sistem keamanan, khususnya pada sistem keamanan *cloud storage* merupakan hal yang harus dilakukan sebagai penelaahan dari kajian-kajian yang telah dilakukan sebelumnya.

ISSN: 2598-8565 (media cetak)
ISSN: 2620-4339 (media online)

DAFTAR PUSTAKA

Cloudraya. (2020). Menjaga Keamanan Data pada Cloud. Retrieved from Cloudraya.com website: https://cloudraya.com/blog/menjaga-keamanan-data-pada-cloud/

Colburn, T. (2013). *Philosophy and computer science*. Oxford: Routledge.

Fachruddin, S. (2016). *Pengantar Filsafat Ilmu*. Bandung: IPB Press Printing.

Ginting, P., & Situmorang, S. H. (2008). *Filsafat Ilmu dan Metode Riset* (Edisi Pert). Medan: USUPress.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*.

Riyanto, G. P. (2021). Data 533 Juta Pengguna Facebook Bocor, Termasuk Indonesia. *Kompas.Com*. Retrieved from https://tekno.kompas.com/read/2021/04/04/09330067/data-533-juta-pengguna-facebook-bocor-termasuk-indonesia

Stallings, W., & Brown, L. (2018). *Computer Security Principles and Practice*. New York: Pearson Education.

Sugiyono. (2013). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitaif, dan R&D*. Bandung: Alfabeta.