KOMPUTASI AWAN

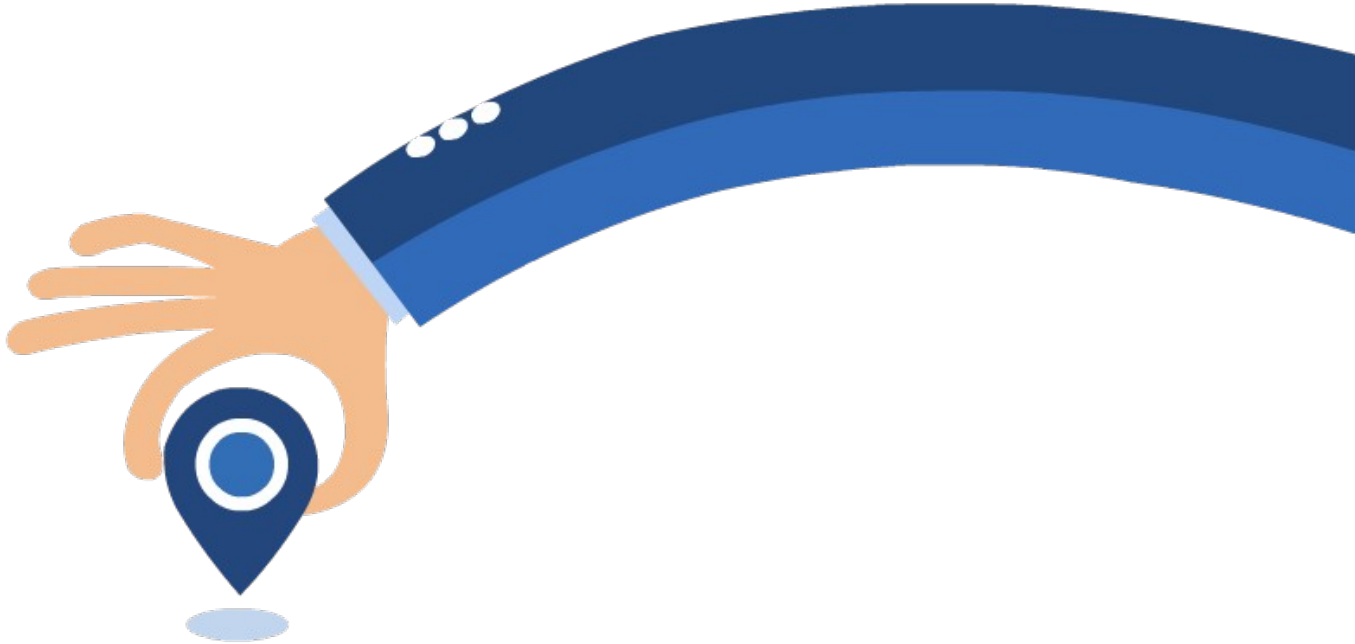
Pertemuan ke-5

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id

السلام عليكم

Wahyu Januar A


0838-1934-7140


wahyu.pyan88@gmail.com


Wahyu Pyan


wahyu_pyan

Petemuan 5 Komputasi Awan

- Model Keamanan Komputasi Awan
- Vendor PaaS, Saas & IaaS

Keamanan Komputasi Awan

Meskipun virtualisasi dan komputasi awan dapat membantu perusahaan mencapai atau melakukan sesuatu yang lebih dengan melanggar ikatan fisik antara infrastruktur IT dan penggunanya, ancaman keamanan yang tinggi harus diatasi dalam rangka untuk mendapatkan manfaat sepenuhnya dari paradigma komputasi baru. Hal ini terutama berlaku untuk penyedia SaaS.

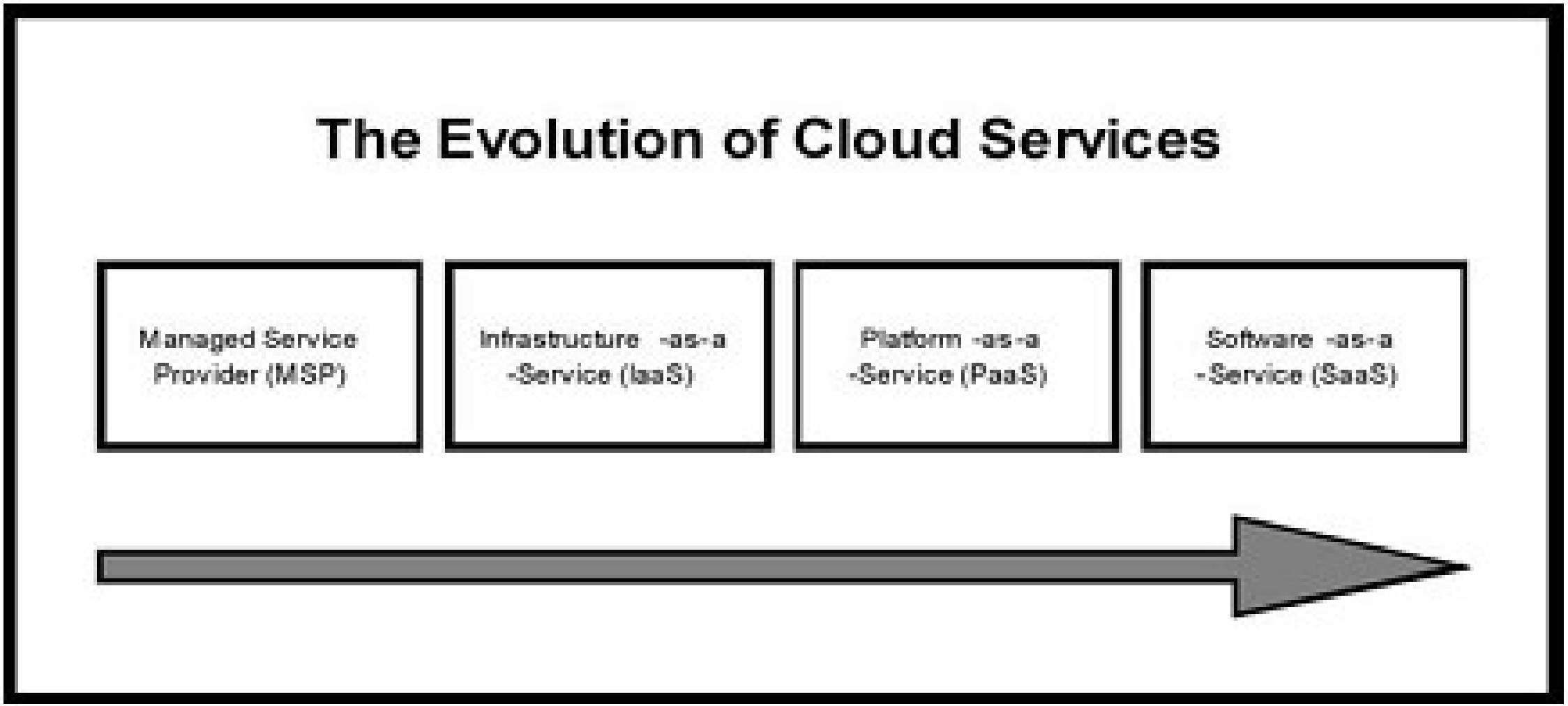
Keamanan Komputasi Awan

Disini akan diambil contoh keamanan pada Layanan SaaS (Software as a Service). Model Cloud computing masa depan kemungkinan besar akan menggabungkan penggunaan SaaS, utilitas komputasi, dan kolaborasi teknologi Web 2.0 untukmemanfaatkan Internet untuk memenuhi kebutuhan pelanggan mereka.

Keamanan Komputasi Awan

Model bisnis baru yang dikembangkan sebagai hasil dari peralihan ke Cloud Computing tidak hanya menciptakan teknologi baru dan proses operasional bisnis tetapi juga persyaratan keamanan baru dan tantangan yang baru. Sebagai langkah evolusi terbaru dalam model layan Cloud (seperti gambar di bawah ini), SaaS kemungkinan akan tetap menjadi model layanan awan yang dominan untuk masa yang akan datang dan sebagai tempat kebutuhan yang paling penting untuk praktik keamanan dan pengawasan

Evolusi Layanan Komputasi Awan



Keamanan Komputasi Awan

Seperti halnya dengan penyedia layanan yang diatur, perusahaan atau pengguna akhir perlu kebijakan penelitian vendor pada keamanan data sebelum menggunakan jasa vendor untuk menghindari kehilangan atau tidak dapat mengakses data mereka.

Analis teknologi dan perusahaan konsultan Gartner mendaftar tujuh isu keamanan yang mana salah satu diantaranya harus dibahas dengan perusahaan Cloud Computing:

7 Isu Keamanan menurut Gartner

- Hak istimewa dari pengguna akses.

  Menanyakan tentang siapa yang memiliki akses khusus untuk data, dan tentang pengangkatan dan pengelolaan administrator tersebut.

- Peraturan kepatuhan.

  Pastikan bahwa vendor bersedia untuk menjalani audit eksternal dan / atau sertifikasi keamanan.

7 Isu Keamanan menurut Gartner

- Lokasi data. Apakah penyedia layanan dalam hal ini perusahaan Cloud Computing melakukan pengendalian terhadap lokasi data..
- Pembagian / pemisahan data.

  Pastikan bahwa enkripsi tersedia di semua tahapan, dan bahwa skema enkripsi dirancang dan diuji oleh para profesional berpengalaman.

7 Isu Keamanan menurut Gartner

- Pemulihanan / pembaruan.

  Cari tahu apa yang akan terjadi pada data sewaktu terjadi bencana / kerusakan. Mereka menawarkan pemulihan lengkap? Jika demikian, berapa lama waktu yang dibutuhkan untuk pemulihan tersebut sehingga pengguna layanan dapat menerima / mengambil data mereka sesuai kebutuhan denganm cepat dan tepat.

7 Isu Keamanan menurut Gartner

- Bantuan investigasi / bantuan penyelidikan.

  Apakah vendor memiliki kemampuan untuk menyelidiki setiap kegiatan yang tidak patut atau ilegal ?

- Kelayakan/kelangsungan jangka panjang.

  Apa yang akan terjadi pada data jika perusahaan yang bersangkutan (vendor) keluar/berhenti dari bisnis? Bagaimana data yang dikembalikan, dan dalam format apa?

Keamanan Komputasi Awan

Menentukan jaminan keamanan data untuk jaman sekarang (hari-hari ini) begitu sulit, sehingga fungsi keamanan data menjadi begitu penting dibandingkan masa lalu. Taktik yang tidak terhandle oleh Gartner adalah meng-enkripsi data diri anda. Jika Anda mengenkripsi data menggunakan algoritma yang terpercaya, maka terlepas dari keamanan penyedia layanan dan kebijakan enkripsi, data hanya akan dapat diakses dengan kunci dekripsi.

Masalah Keamanan Data Komputasi Awan

- Masalah keamanan dari Virtual machine.

  Apakah Blue Cloud IBM atau Windows Azure di Microsoft, teknologi mesin virtual dianggap sebagai platform komputasi awan dari komponen fundamental, perbedaan antara Blue Cloud dan Windows Azure adalah bahwa virtual mesin berjalan pada sistem operasi Linux atau sistem operasi Microsoft Windows. Teknologi virtual mesin membawa keuntungan yang nyata, ini memungkinkan pengoperasian server tidak lagi bergantung pada perangkat fisik. Tapi pada server virtual. Pada mesin virtual, perubahan yang fisik terjadi atau migrasi tidak mempengaruhi layanan yang diberikan oleh penyedia layanan.

Masalah Keamanan Data Komputasi Awan

- Keberadaan super user.

  Untuk perusahaan yang menyediakan layanan komputasi awan (Cloud Computing), mereka memiliki hak untuk melaksanakan pengelolaan dan pemeliharaan data, adanya superuser sangat bermanfaat untuk menyederhanakan fungsi manajemen data, tetapi merupakan ancaman serius bagi pengguna pribadi.

Masalah Keamanan Data Komputasi Awan

Bukan hanya pengguna individu tetapi juga organisasi memiliki potensi ancaman serupa, misalnya pengguna korporat dan rahasia dagang disimpan dalam platform komputasi awan mungkin dicuri. Oleh karena itu penggunaan hak super user harus dikendalikan di awan (Cloud).

Masalah Keamanan Data Komputasi Awan

- Konsistensi data.

  Lingkungan Awan (Cloud) merupakan lingkungan yang dinamis, dimana data pengguna mentransmisikan data dari data center kepengguna. Untuk sistem, data pengguna berubah sepanjang waktu. Membaca dan menulis data berkaitan dengan identitas otentikasi pengguna dan hal perijinan.

Masalah Keamanan Data Komputasi Awan

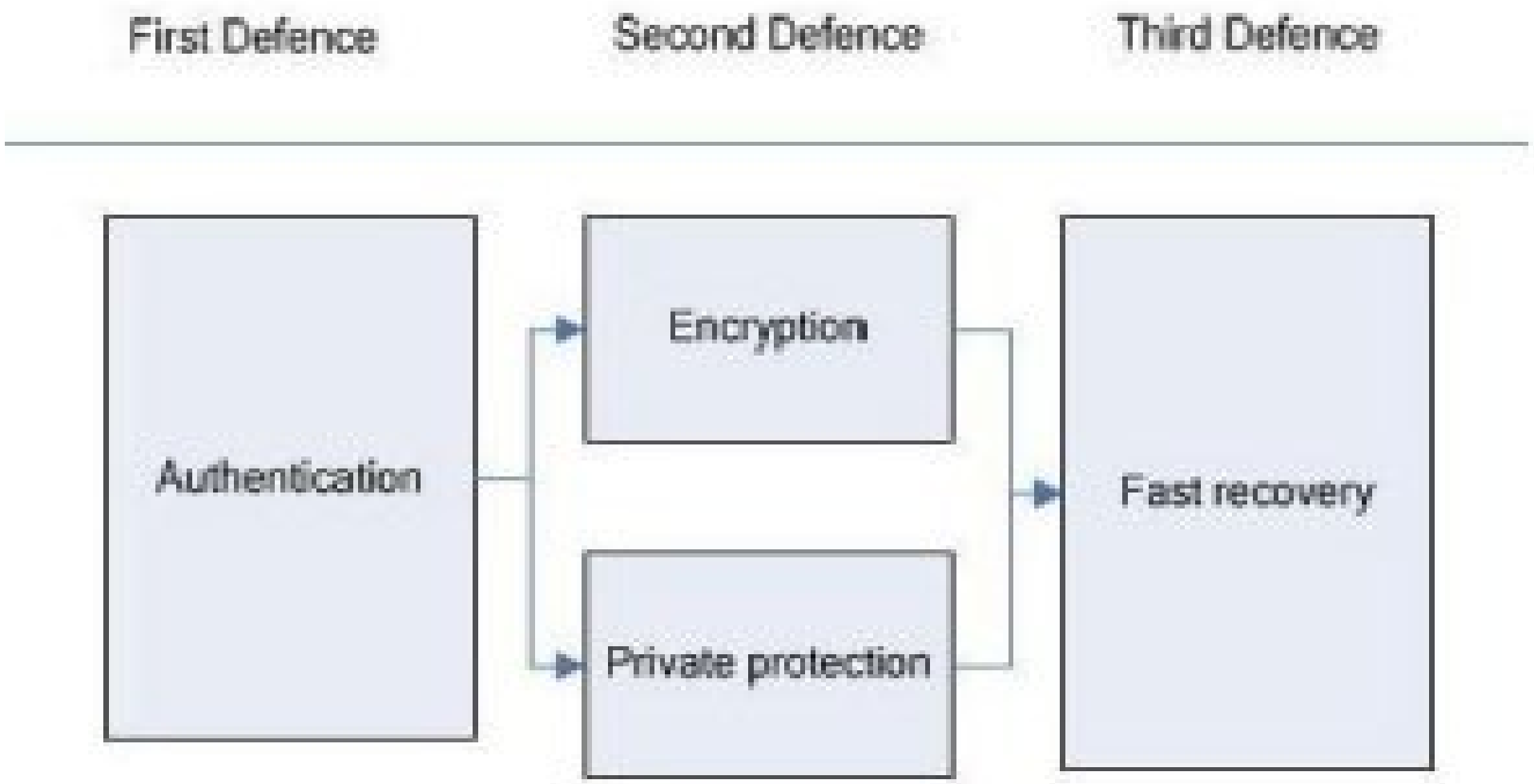
Membaca dan menulis data berkaitan dengan identitas otentikasi pengguna dan hal perijinan. Dalam sebuah mesin virtual, mungkin ada data pengguna yang berbeda yang harus wajib dikelola. Model kontrol akses tradisional

dibangun di “tepi” komputer, sehingga sangat lemah untuk mengendalikan pembaca dan penulis di antar komputer yang terdistribusi.

Prinsip Keamanan Data Komputasi Awan

Semua teknik keamanan data dibangun pada kerahasiaan, integritas dan ketersediaan dari tiga prinsip dasar. Kerahasiaan mengacu pada apa yang disebut dengan data aktual atau informasi yang tersembunyi, terutama pada daerah yang sensitive, kerahasian data berada pada persyaratan yang lebih ketat. Untuk komputasi awan, data disimpan di "pusat data", keamanan dan kerahasiaan data pengguna, merupakan hal yang penting

Model Keamanan Data Komputasi Awan



Model Keamanan Data Komputasi Awan

Model struktur yang digunakan adalah system pertahanan tiga tingkat. di mana setiap tingkat melakukan tugas masing-masing untuk memastikan keamanan data dari lapisan awan (cloud).

- Lapisan Pertama bertanggung jawab untuk otentikasi pengguna, pengguna sertifikat digital yang diterbitkan oleh yang sesuai/berwenang, mengatur hak akses pengguna.

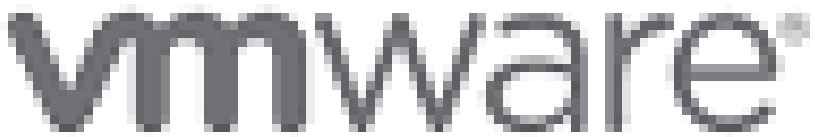
Model Keamanan Data Komputasi Awan

- Lapisan Kedua : bertanggung jawab untuk enkripsi data pengguna, dan melindungi privasi dari pengguna melalui cara tertentu;
- Lapisan Ketiga : Data pengguna untuk pemulihan sistem yang cepat, perlindungan sistem lapisan terakhir dari data pengguna.

Vendor Software as a service (Saas)

Vendor Platform as a service (Paas)

Vendor Infrastruktur as a service (Iaas)



Terima Kasih

Tugas

- Buatlah Slide Presentasi Tentang Aplikasi Cloud Storage
  1. Amazon / AWS (cloud drive)
  2. One Drive
  3. Google Drive
  4. Dropbox
  5. Mega
  6. Mediafire

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id