KEAMANAN DATA PADA "TORNADO" SISTEM MULTI KOMPUTASI AWAN MENGGUNAKAN DATA MINING DETECTION MALWARE

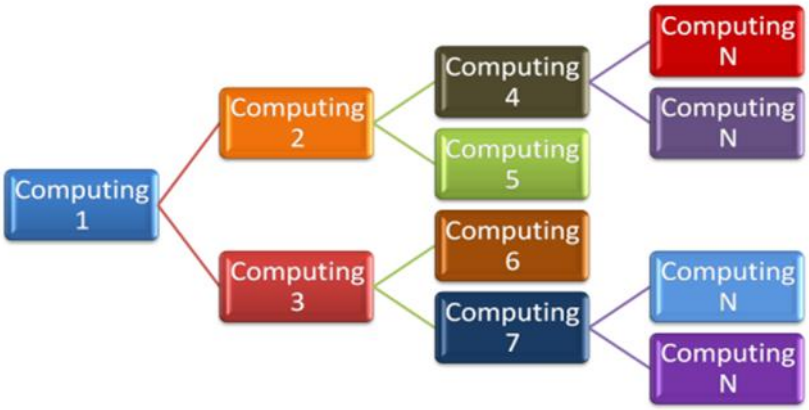
Maya Hilda Lestari Louk
Teknik Informatika, Universitas Surabaya
E-mail: mayalouk@staff.ubaya.ac.id

Abstract.
The use of cloud computing technology has been increasing in many ways. Cloud computing is not only used by private individual but also by company or organization with big data maintenance and processing. One cloud computing is not sufficient to handle our needs. Thus, multi clouds ideas is a solution to handle and maintain enormous data. This paper proposes the idea of multi clouds architecture which is more efficient and secure to maintain the so called "Tornado" multi clouds computing**.** Security system contains activities monitor, detection and recorder then communication handler will be notified to user. According to the analysis of the system, it will be a new solution for a more secure multi clouds.

Keywords: Architecture, Big Data, Cloud Computing, Communication Handler Notification, Detecting Recording Tornado Multi Clouds

PENDAHULUAN

Strategi multi komputasi awan adalah penggunaan dua atau lebih layanan komputasi awan secara bersamaan untuk meminimalkan risiko kehilangan atau downtime data yang luas karena kegagalan komponen yang dilokalkan dalam lingkungan komputasi awan. Kegagalan seperti itu dapat terjadi pada perangkat keras, perangkat lunak, atau infrastruktur. Strategi multi komputasi awan juga dapat meningkatkan kinerja perusahaan secara keseluruhan dengan menghindari "vendor lock-in" dan menggunakan infrastruktur yang berbeda untuk memenuhi kebutuhan beragam mitra dan pelanggan. Ada banyak kemungkinan kegagalan yang mungkin terjadi dalam komputasi awan.



Gambar 1 Outline "Tornado" Sistem Multi Komputasi Awan

Menurut gambar 1 warna berbeda diberikan kepada penyedia yang berbeda atau nama pengguna yang berbeda di bawah tingkat otorisasi yang sama. Sistem Multi Komputasi Awan "Tornado" tidak hanya memberikan pengarahan data cadangan atau sistem cadangan tetapi juga solusi untuk mengatur penyebaran data dan sistem komputasi. Kesimpulannya, sistem tornado akan berada pada satu paket dengan sistem pemantauan dan keamanan untuk membuatnya lebih aman dan lebih efisien bagi konsumen.

Challenges Issues pada Sistem Multi Komputasi Awan

Menurut *top threats working group, the notorious nine cloud computing top threats* yang dirilis pada Februari 2013 oleh aliansi keamanan cloud; ancaman komputasi awan adalah: Pelanggaran Data, Kehilangan Data, Pembajakan Akun, Insecure API, Penolakan Layanan, Orang Dalam yang Berbahaya, Penyalahgunaan Layanan Komputasi Awan, Uji Tuntas yang Tidak Memadai, Masalah Teknologi Bersama. Akar semua masalah ini bukan di keamanan itu sendiri tetapi dalam proses pemantauan. Pemantauan oleh kedua belah pihak antara konsumen dan penyedia dapat meningkatkan tingkat kerahasiaan. Menurut MODAClouds, Analisis Risiko dan Kualitas dalam Lingkungan Multi-Cloud, ada 3 aspek penting yang harus dipertimbangkan dalam lingkungan multi-cloud:

1. Heterogenitas layanan yang ditawarkan oleh penyedia yang berbeda menghasilkan berkurangnya pertukaran informasi yang tidak diinginkan
2. Migrasi adalah operasi penting untuk memastikan terpenuhinya persyaratan aplikasi
3. Ancaman keamanan meningkat di lingkungan multi komputasi awan. Semua ini dapat terjadi karena migrasi komunikasi antara penyedia komputasi awan yang berbeda dan hal itu menyebabkan banyak penerima data dan membuatnya lebih sulit untuk menjamin kerahasiaan. Masalah atau risiko lain yang diketahui dari lingkungan multi komputasi awan, seperti: Risiko biaya tidak dapat diprediksi, karena menggunakan layanan yang berbeda dari penyedia yang berbeda, hal itu dapat mengakibatkan biaya tak terduga.

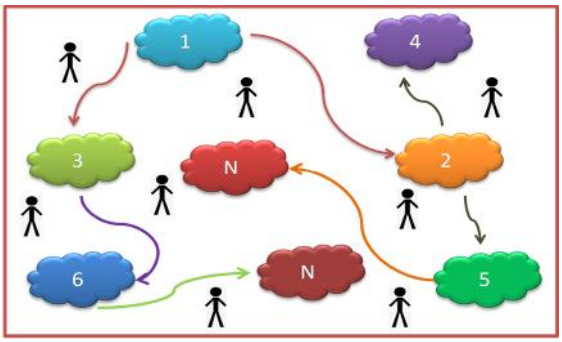
Beberapa tantangan terkait proses migrasi dari satu layanan ke layanan lain yang harus diperhitungkan: [6]

1. Kurangnya kompatibilitas antara berbagai layanan
2. Karena kebutuhan kompatibilitas antara layanan root komputasi awan dan komputasi awan yang baru semakin tinggi semakin mudah migrasi terjadi.
3. Kompleksitas migrasi pengaturan
4. Proses migrasi menjadi rumit dan mahal jika penyesuaian konfigurasi antara dua penyedia komputasi awan terlalu rumit.
5. Proses pengujian yang kompleks
6. Akses mudah ke layanan pengujian dan total waktu henti adalah dua aspek yang akan memengaruhi kompatibilitas migrasi tertentu
7. Kontrak hukum yang tidak ramah migrasi
8. Penyedia cenderung menonaktifkan migrasi untuk mencegah pengguna bermigrasi ke penyedia lain atau hanya menggabungkan dua penyedia yang berbeda
9. Mekanisme replikasi yang kompleks dan tidak efisien
10. Kompleksitas untuk mensinkronkan data antara dua layanan mungkin menghambat kemungkinan ko-eksistensi dan penggunaan layanan baru sebagai cadangan untuk yang pertama menjadi tidak efisien.

Tabel 1 menunjukkan "*Quality of proper indicator*".
Hal ini penting untuk melindungi privasi data dan Identitas. [6]

Security	Possible indicators
Confidentiality	Perjanjian antara penyedia dan pengguna untuk data umum dan privasi identitas dalam multi komputasi awan dan untuk mengisolasi layanan dan *Virtual Machine*
Integrity	Tingkat kesepakatan antara *Cloud Service Provider* tentang mekanisme pelestarian integritas data
Availability	Tingkat kesepakatan antara layanan dalam hal jaminan ketersediaan
Non-Repudiation	Kesepakatan di antara *Cloud Service Provider* untuk memberikan bukti integritas dan asal data.
Accountability	Persyaratan forensik: penyediaan *file log* dan data manajemen dan keamanan
Authorization & Authentication	Adanya mekanisme aman dan disetujui (standar) yang kompatibel untuk otentikasi dan otorisasi pengguna

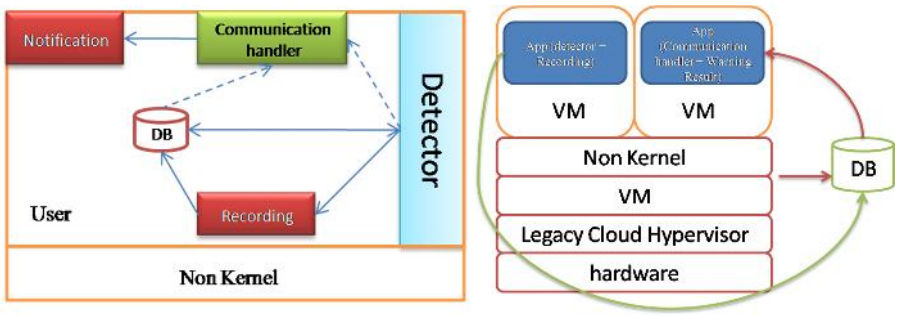
3 Tornado Multi Clouds Design



Gambar 2: Pengguna dan distribusi data "Tornado" sistem multi komputasi awan

Keuntungan dari Tornado Sistem Multi Komputasi Awan:

1. Sistem pemantauan dan keamanan untuk seluruh pemrosesan.
2. Seseorang dapat mengakses cloud melalui cloud induk.
3. Seluruh alamat cloud sistem, kecuali untuk pengguna utama yang dapat diacak. Oleh karena itu pengguna kedua dibatasi untuk menggunakan cloud hanya satu induk.
4. Fungsi komputasi dan distribusi data dapat ditetapkan.



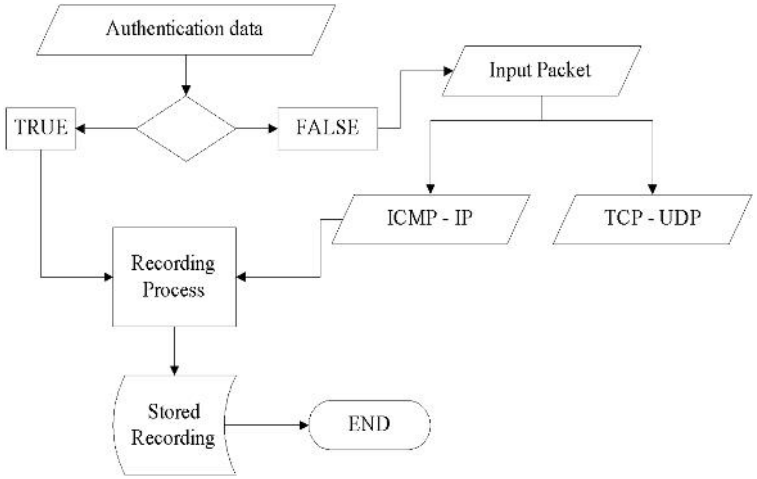
Gambar 3: Sistem Keamanan dengan Non-Kernel "Tornado" sistem multi komputasi awan

Detektor aktivitas masuk tidak diperlihatkan di layar karena itu penyusup mungkin tidak mengetahui keberadaannya. Detektor akan mencatat semua informasi tentang penyusup. Semua sistem perekaman akan dikirim ke basis data, dan akhirnya basis data akan memberikan file rekaman ke pengendali komunikasi untuk memprosesnya dan memberikan pernyataan hasil dalam dua tingkat peringatan: hijau dan merah. Di mana merah adalah situasi berbahaya, hasil pelacakan menunjukkan bahwa itu adalah login ilegal, dan hijau berarti itu adalah login pengguna yang legal. Pernyataan atau pemberitahuan hasil tidak hanya memberitahu itu legal atau ilegal tetapi juga kegiatan apa pun selama proses akses. Sistem otentikasi akan disematkan dengan One Time Password

(OTP) yang akan dikirim melalui Short Message Service (SMS) untuk mengaktifkan login. Penggunaan sistem non Kernel adalah ide yang efektif dan efisien untuk melindungi sistem komputasi awan tanpa banyak usaha dari penyedia. Pengguna akan diaktifkan untuk memulai sistem keamanan dengan sendirinya. Non-kernel adalah hybrid kernel / hypervisor yang dirancang untuk memenuhi ketiga persyaratan fungsional yang disebutkan di bagian sebelumnya: ini memungkinkan optimasi dua tujuan dari pekerjaan yang berguna dan biaya; mengekspos sumber daya dan biayanya langsung ke aplikasi; dan mengisolasi aplikasi dari satu sama lain. [3]

4 Sistem Keamanan

Detector – Recorder



Gambar 4: Flow Chart Sistem Keamanan "Tornado" Sistem Multi Komputasi Awan

Dengan sistem semacam ini, seseorang dapat menangani data yang sangat besar dengan lebih cepat. Jika tuan rumah menjadi korban penyerang dan mengendalikan system. Sistem pada tuan rumah itu akan dikompromikan. Dalam kasus seperti itu, penyerang tidak akan membiarkan sistem mengirim peringatan kepada administrator dan dapat memainkan malapetaka dengan data dan aplikasi.

Communication Handler – Notification

Notification handler komunikasi harus dapat menjangkau pengguna *smartphone*. Tindakan yang direkam harus segera dibaca. Pengguna dapat menggunakan NotificationCompat.Builder untuk menyesuaikan notifikasi pada aplikasi android di mana pembangun dapat memanggil ID Notifikasi tertentu dengan Notification Manager.notify (ID, notifikasi). Jika pemberitahuan sebelumnya masih terlihat, sistem memperbaruinya dari konten objek Pemberitahuan. Jika pemberitahuan sebelumnya telah ditolak, notifikasi baru dibuat sebagai gantinya.

KESIMPULAN

Seluruh sistem Tornado efisien dan efektif untuk menangani kebutuhan data yang sangat besar. Sistem ini juga diperkuat menggunakan otentikasi OTP dan detektor-perekam dan pemberitahuan handler-komunikasi. Gagasan yang diusulkan akan ditujukan untuk aplikasi *mobile*. Aktivitas saat ini dari sistem multi cloud akan selalu dikirim ke pengguna yang sah melalui pembaruan notifikasi. Dalam waktu dekat, sistem aplikasi seluler untuk melacak penyusup sedang dikembangkan.

DAFTAR PUSTAKA

1. Paxson, Vern. 1999. "Bro: a system for detecting network intruders in real-time."*Computer networks* 31.23, 2435-2463.
2. Gul, Irfan, and M. Hussain. 2011. "Distributed cloud intrusion detection model."*International Journal of Advanced Science and Technology* 34, 71-82.
3. Ben-Yehuda, Muli, et al. 2013. "The nonkernel: a kernel designed for the cloud."*Proceedings of the 4th Asia-Pacific Workshop on Systems*. ACM.
4. Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. 2009. "Towards trusted cloud computing." *Proceedings of the 2009 conference on Hot topics in cloud computing*.
5. Ramgovind, S., Mariki M. Eloff, and E. Smith. *2010.* "The management of security in cloud computing." *Information Security for South Africa (ISSA)*. IEEE, 2010.
6. Omerovic, Aida, Victor Muntés Mulero, and Peter Matthews. 2013. "Risk and Quality Analysis in Multi-Cloud Environments.".