ANALISIS METODE PENGAMANAN DATA PADA LAYANAN *CLOUD COMPUTING*

Munirul Ula [1]
Program Studi Sistem Informasi Fakultas Teknik
Universitas Malikussaleh
nanggroe@gmail.com [1]

Abstrak

Abstrak— Saat ini layanan *cloud computing* sudah menjadi bagian dari system informasi yang lumrah digunakan pada perusahaan *modern*. Hal ini dipicu oleh biaya yang relative murah, *reliable* dan effisien. Akan tetapi cloud computing memiliki banyak masalah keamanan yang menjadi perhatian besar saat ini, yaitu cara perlindungan data, keamanan jaringan, keamanan virtualisasi, integritas aplikasi, dan manajemen identitas yang digunakan oleh layanan *cloud computing* tersebut. Masalah perlindungan data adalah salah satu masalah keamanan yang paling penting, karena sebuah organisasi atau perusahaan tidak akan mentransfer datanya ke tempat penyimpanan jika tidak ada perlindungan data yang baik dari penyedia layanan *cloud*. Banyak metode yang disarankan untuk perlindungan data dalam cloud computing, namun masih banyak kelemahannya. Metode Pengamanan yang paling populer meliputi SSL (*Secure Socket Layer*) Enkripsi, Intrusion *Detection System*; *Multi Tenancy Based Access Control*, dll. Tujuan makalah ini adalah untuk menganalisis dan mengevaluasi metode pengamanan terpenting untuk perlindungan data dalam *cloud computing*. Selanjutnya, untuk meningkatkan keamanan data, beberapa metode pengamanan untuk perlindungan data akan direkomendasikan untuk diaplikasikan pada layanan *cloud computing*.

Kata Kunci : kontrol akses, otentikasi, otorisasi, *cloud computing*, kerahasiaan, perlindungan data.

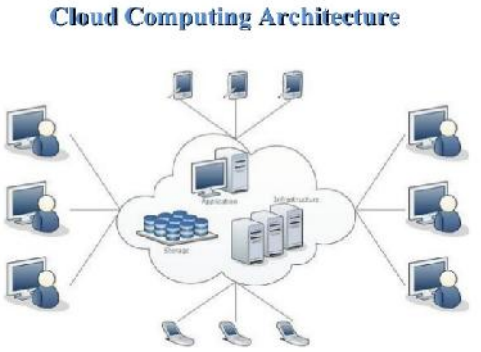
DOI: https://doi.org/10.29103/techsi.v11i1.1357

1. Pendahuluan

Cloud Computing adalah sekelompok komputer yang digunakan bersama untuk menyediakan layanan perhitungan atau tugas yang berbeda beda. *Cloud Computing* adalah salah satu paradigma TI yang paling penting dalam beberapa tahun terakhir. Salah satu manfaat utama yang ditawarkan dari teknologi IT ini bagi perusahaan adalah mengurangi waktu dan biaya dikeluarkan oleh perusahaan untuk mengelola system informasi. *Cloud Computing* memberikan layanan untuk perusahaan atau organisasi untuk menggunakan media penyimpanan dan daya komputasi secara bersama-sama. Ini lebih baik daripada perusahaan mengembangkan dan beroperasi dengan infrastruktur mereka sendiri. *Cloud Computing* juga menyediakan infrastruktur TI yang fleksibel, aman, dan hemat biaya. Hal ini dapat dibandingkan dengan jaringan listrik nasional yang memungkinkan organisasi dan rumah untuk terhubung ke sumber energi terpusat, efisien dan hemat biaya. Perusahaan besar di dunia seperti Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, dan Novell telah berinvestasi dalam *Cloud Computing* dan menawarkan berbagai solusi berbasis cloud untuk individu dan dunia bisnis.

Ada berbagai jenis dan model *Cloud Computing* yang menawarkan berbagai layanan yang diberikan; yaitu, *public cloud*, *private cloud*, *hibrid cloud*, dan *community cloud*. Dari segi model pengiriman, layanan *cloud* dapat dikategorikan sebagai SaaS (Perangkat Lunak sebagai layanan), PaaS (*Platform* sebagai Layanan), dan IaaS (*Infrastructure as a Service*). *Cloud Computing* biasanya dikelompokkan dengan dua cara: berdasarkan lokasi *Cloud Computing*, dan berdasakan jenis layanan yang ditawarkan.

DOI: https://doi.org/10.29103/techsi.v11i1.1357



Gambar 1: Arsitektur *Cloud Computing*

Berdasakan lokasi *Cloud, Cloud Computing* biasanya diklasifikasikan sebagai: *public cloud* (di mana infrastruktur komputasi dipandu oleh vendor *cloud*); *Private cloud* (di mana infrastruktur komputasi ditugaskan ke organisasi tertentu dan tidak dibagi dengan organisasi lain); *Hibrid cloud* (penggunaan *private cloud* dan *public* secara bersama-sama); Dan *community cloud* (ini melibatkan pembagian infrastruktur TI di antara anggota organisasi komunitas yang sama) [1]. Berdasarkan pada jenis layanan yang ditawarkan, *cloud* diklasifikasikan sebagai berikut: IaaS (Infrastruktur sebagai layanan), PaaS (Platform sebagai Layanan), dan Perangkat Lunak sebagai Layanan (SaaS) [1].

2. Jenis Serangan Terhadap *Cloud Computing* Jenis Serangan Terhadap *Cloud Computing*

Cloud Computing sebagai teknologi baru untuk memproses dan mentransfer data secara elektronik saat ini digunakan di hampir semua sistem komputer. Ini berjalan pada infrastruktur jaringan yang dibuka untuk berbagai jenis serangan. DDoS (*Distributed Denial of Service*) adalah salah satu serangan yang paling dikenal yang digunakan pada *cloud computing*. Dengan mensinkronisasi cookie serta pembatasan pengguna yang terhubung dengan teknologi *cloud* ke server dapat digunakan sebagai tindakan untuk menghentikan Distributed Denial of Service[2]. Jenis serangan lainnya pada teknologi *cloud computing* adalah man in the middle

DOI: https://doi.org/10.29103/techsi.v11i1.1357

attach. Secure Socket Layer (SSL) adalah metode pengamanan untuk mengatasi serangan semacam ini. Jadi, jika metode pengamanan ini tidak terkonfigurasi dengan benar, otentikasi klien dan server mungkin tidak berjalan sebagaimana mestinya untuk melindungi pengguna layanan cloud dari penyerang yang menggunakan teknik *man in the middle attack*. Oleh karena itu tantangan keamanan dalam melindungi data saat menggunakan cloud computing harus dipecahkan dan diminimalisir dengan tepat. Saat kita menggunakan cloud computing kita menjalankan software kita pada hard disk dan CPU yang tidak ada di depan kita. Itulah sebabnya pengguna memiliki lebih banyak keraguan tentang masalah keamanan saat mereka menggunakan teknologi ini. Jadi, banyak jenis serangan yang berbeda bisa terjadi pada teknologi cloud. Selain itu, serangan yang paling dikenal meliputi phishing, spoofing IP, modifikasi pesan, analisis lalu lintas, port IP, dll [2].

3. Metode Pengamanan untuk Cloud Computing

Ada beberapa metode pengamanan untuk perlindungan data yang diterima dari penyedia Cloud Computing, dan semuanya harus memiliki otentikasi, kerahasiaan, kontrol akses dan otorisasi.

A. Otentikasi dalam Cloud Computing

Otentikasi dalam Cloud Computing untuk memastikan bahwa orang yang tepat mendapatkan akses ke data yang tersedia dari penyedia teknologi cloud. Saat otentikasi dipastikan dalam Cloud Computing, artinya identitas pengguna dibuktikan ke penyedia layanan cloud computing saat mengakses informasi tersimpan di cloud. Jenis public cloud dan private menggunakan berbagai desain untuk otentikasi dengan RSA. Kriptosistem RSA menerima model yang berbeda untuk otentikasi seperti autentikasi dua faktor, otentikasi berbasis pengetahuan, dan otentikasi adaptif. AWS (Amazon Web Services) terkonsentrasi pada transfer informasi rahasia antara server web dan browser termasuk private cloud virtual [3]. Dalam konteks ini, skema otentikasi yang berbeda diterapkan, seperti otentikasi multifaktor, manajemen akses, dan identitas AWS. Gambar 1 menyajikan prosedur otentikasi multifaktor dari AWS. Ada juga metode untuk

DOI: https://doi.org/10.29103/techsi.v11i1.1357

otentikasi yang memungkinkan pengguna menggunakan hanya satu kata sandi untuk mengotentikasi dirinya ke beberapa layanan [4]. Dengan metode ini pengguna rentan terhadap serangan honeypot dan dictionary. Perusahaan IT yang paling terkenal menggunakan metode ini seperti Google, Microsoft, dan Facebook. Untuk mengaktifkan otentikasi alamat IP yang diperlukan ke beberapa situs eksternal saat Cloud Computing digunakan, pengaturan proxy dapat digunakan. URL proxy hanya memungkinkan situs terpercaya untuk diakses [5].

Oleh karena itu, kita dapat menyimpulkan di sini bahwa untuk perlindungan data dari teknologi cloud mekanisme otentikasi yang paling banyak digunakan adalah: otentikasi berbasis pengetahuan, autentikasi dua faktor, otentikasi adaptif, otentikasi multifaktor dan otentikasi kata kunci tunggal. Otentikasi berbasis pengetahuan, autentikasi dua faktor dan otentikasi adaptif diaktifkan dengan RSA dan manfaatnya mengurangi biaya dan keamanan yang lebih baik. Autentikasi multifaktor digunakan oleh AWS untuk mengamankan data di cloud. Manfaat dari mekanisme otentikasi ini adalah memungkinkan pengelolaan identitas dan manajemen akses. Otentikasi kata sandi tunggal digunakan dari Facebook untuk mengaktifkan perlindungan data di cloud. Manfaat mekanisme otentikasi semacam ini adalah memungkinkan keamanan dari serangan honeypot dan serangan kamus [5].

B. Kerahasian dalam Cloud Computing

Kerahasiaan adalah salah satu mekanisme keamanan yang paling penting untuk perlindungan data pengguna di cloud. Ini mencakup enkripsi plaintext dalam teks sandi sebelum data disimpan di cloud. Metode ini melindungi data pengguna dan bahkan penyedia layanan cloud computing tidak dapat memodifikasi atau membaca konten yang disimpan di cloud. Proteksi semacam ini ditawarkan dari perlindungan data Dell dan enkripsi dimana data pengguna dilindungi saat disimpan di drive eksternal atau media. Enkripsi bisa dilakukan baik dengan menggunakan software maupun hardware [5]. Manfaat besar dari perlindungan semacam ini adalah pengguna tidak perlu repot-repot menerapkan kebijakan proteksi dan enkripsi data Dell. Dell

DOI: https://doi.org/10.29103/techsi.v11i1.1357

juga menggunakan Transparent File Encryption untuk mengendalikan pengguna yang mengakses data. Wuala cloud adalah vendor lain yang memungkinkan enkripsi untuk data di cloud. Enkripsi diaktifkan di sini sebelum komputer pribadi mengirimkan data ke cloud. Ini adalah perlindungan yang sangat baik karena bahkan provider pun tidak bisa mengakses data. Penulis dalam [6] mengusulkan metode enkripsi untuk Cloud Computing yang didasarkan pada atribut hirarkis. Metode pengamanan yang disarankan untuk kerahasiaan dalam Cloud Computing ini memberikan kinerja dan kontrol akses yang sangat baik. Penulis dalam [7] mengusulkan metode enkripsi dimana pemilik dapat mengendalikan data yang mereka miliki di cloud.

Kerahasiaan juga disediakan oleh vendor cloud Online Tech yang mendapatkan kerahasiaan dalam Cloud Computing dengan menggunakan metode enkripsi (seperti Full Disk Encryption) yang mengenkripsi data tersimpan pada hard disk selama proses booting. Enkripsi Disk secara utuh juga digunakan untuk mengenkripsi data dengan algoritma AES (Advanced Encryption Standard) yang terkenal. Jika perangkat yang menggunakan teknologi cloud computing hilang atau dicuri, maka ada password pengunci yang melindungi data pada perangkat yang hilang atau dicuri. Online Tech menawarkan Enkripsi Disk Penuh dan Enkripsi Disk Utuh untuk memungkinkan kerahasiaan data di cloud. Manfaat dari metode enkripsi ini adalah bahwa data yang dipartisi dapat didekripsi dan data dienkripsi pada saat tidak digunakan [8]. Oleh karena itu, dapat disimpulkan di bagian ini, bahwa kerahasiaan sangat penting untuk melindungi data di cloud dan vendor yang berbeda menawarkan metode pengamanan yang berbeda untuk memastikan kerahasiaan. Contohnya, DELL (www.dellemc.com) menawarkan enkripsi berbasis perangkat keras dan perangkat lunak, serta enkripsi file tersendiri. Manfaat dari metode enkripsi semacam ini adalah bahwa mereka mudah diterapkan dan tidak diperlukan intervensi dari pengguna.

C. Kontrol Akses di Cloud Computing

Kontrol akses adalah mekanisme keamanan yang sangat penting untuk memungkinkan perlindungan data dalam Cloud

DOI: https://doi.org/10.29103/techsi.v11i1.1357

Computing. Ini memastikan bahwa hanya pengguna resmi yang memiliki akses ke data yang diminta yang tersimpan di cloud. Ada berbagai metode pengamanan yang memungkinkan kontrol akses yang tepat dalam Cloud Computing. Instrution Detection System, firewall serta pengaturan previlege dapat diimplementasikan pada lapisan jaringan dan cloud yang berbeda. Firewall bisa disetting hanya mengaktifkan konten yang disaring untuk melewati jaringan cloud. Firewall biasanya dikonfigurasi sesuai dengan kebijakan keamanan yang ditentukan oleh pengguna. Firewall biasanya berhubungan dengan zona demiliterisasi (DMZ) yang memberikan keamanan data tambahan [9].

McAfee adalah vendor yang menyediakan kontrol akses dalam Cloud Computing. McAfee ini menawarkan metode yang berbeda beda untuk kontrol akses yaitu McAfee Single Sign On, McAfee Web Gateway, dan McAfee satu kali kata sandi (www.mcafee.com). Metode pengamanan jenis ini memungkinkan pengelolaan kebijakan keamanan untuk pencegahan data hilang. Fujitsu adalah vendor lain yang menawarkan kontrol akses dengan berbagai metode otorisasi seperti Virtual System Management dan Central Management Authorization (www.fujitsu.com). Metode pengamanan ini efektif untuk mencegah serangan cross-site scripting dan injeksi [10].

D. Otorisasi di Cloud Computing

Otorisasi dalam Cloud Computing penting bagi pengguna saat mereka masuk ke beberapa layanan cloud computing. Otorisasi biasanya digunakan setelah proses otentikasi. Oracle Database Vault adalah contoh metode pengamanan yang memungkinkan otorisasi di cloud. Metode pengamanan ini ditawarkan oleh vendor Oracle. Data aplikasi dari pengguna administratif yang berbeda dilindungi dengan metode otorisasi ini. Pengguna menggunakan metode otorisasi berdasarkan kebijakan yang melindungi privasi pengguna yang memungkinkan mereka menetapkan kebijakan privasi sendiri. Dengan cara ini pengguna melindungi datanya dengan cara yang efektif dari akses yang tidak sah [11].

DOI: https://doi.org/10.29103/techsi.v11i1.1357

Otorisasi di cloud juga ditawarkan oleh VMware yang mengintegrasikan kebijakan penyedia layanan dengan direktori perusahaan dan kebijakan yang berbeda. Sertifikat atau token lunak digunakan untuk memberi otorisasi kepada pengguna akhir secara aman. Otorisasi OASIS Cloud memungkinkan metode pengamanan berdasarkan pengelolaan otorisasi. Pengguna log dipelihara dengan metode ini yang memberi lokasi pengguna dan informasi tentang perangkat yang digunakan dari pengguna.

4. Rekomendasi untuk Peningkatan Keamanan Data dalam Cloud Computing

Penulis akan menyebutkan sekarang rekomendasi yang paling penting agar memiliki lingkungan cloud yang aman. Salah satu rekomendasinya adalah konsumen cloud harus memastikan bahwa proses tata kelola, risiko dan kepatuhan yang efisien ada. Ini berarti bahwa kontrol keamanan harus ada dalam Cloud Computing yang serupa dengan sistem TI tradisional. Bagaimanapun, Cloud Computing mungkin memiliki risiko berbeda bagi organisasi daripada solusi TI tradisional. Jadi, ketika organisasi menggunakan Cloud Computing, sangat penting konsumen untuk memahami tingkat toleransi risiko [12].

Rekomendasi lainnya adalah penyedia layanan cloud computing harus memiliki fungsi dan proses yang jelas untuk pengelolaan akses ke aplikasi dan data konsumen. Hal ini penting untuk memastikan bahwa akses ke lingkungan cloud dikelola dan dikendalikan. Jadi pengelolaan hak access dan identitas pengguna layanan sangat penting untuk diterapkan di lingkungan cloud. Ketika suatu perusahaan konsumen mulai mengunakan layanan cloud, akan sangat penting untuk memungkinkan konsumen menetapkan identitas pengguna mereka ke dalam kelompok dan tingkatan akses yang mencerminkan kebijakan keamanan pada bisnis operasional mereka [13].

Faktor yang juga sangat penting untuk lingkungan cloud yang aman adalah adanya jaminan perlindungan data dan informasi yang memadai. Pertimbangan keamanan harus diterapkan pada data yang tersimpan dalam beberapa bentuk sistem penyimpanan, serta untuk data yang ditransfer melalui beberapa link komunikasi. Data untuk Cloud Computing memiliki

DOI: https://doi.org/10.29103/techsi.v11i1.1357

berbagai macam risiko yaitu risiko pencurian data dan pengungkapan data yang tidak sah, risiko gangguan akses data, dan risiko kehilangan data atau ketidaktersediaan data.

Untuk mengamankan data dalam Cloud Computing diperlukan kontrol yang baik seperti: tool pengaturan privasi, kerahasiaan, pembuatan katalog aset data, integritas dan ketersediaan, serta tool pengatturan identitas dan manajemen akses pengguna [14]. Rekomendasi penting untuk mengamankan data cloud computing adalah dengan memastikan keamanan semua jaringan dan koneksi ke layanan cloud. Konsumen cloud harus melindungi jaringan internal mereka dari serangan internal seperti pengungkapan data rahasia dan privacy, modifikasi data yang tidak sah, atau serangan terhadap ketersediaan data dan akses terhadap layanan cloud. Itulah sebabnya penting bagi konsumen pengguna cloud untuk mengevaluasi kontrol jaringan internal penyedia layanan cloud computing mengenai persyaratan dan kebijakan keamanan yang mungkin dimilikinya. Salah satu rekomendasi utama adalah evaluasi kontrol keamanan terhadap sarana dan prasarana fisik. Konsumen pengguna cloud bertanggung jawab untuk memastikan provider menjaga keamanan dalam cloud computing, seperti infrastruktur dan fasilitas yang dikendalikan dan dimiliki oleh penyedia layanan cloud.

a. Perlindungan Data di Cloud

Perlindungan data di cloud paling baik dilakukan dengan enkripsi data, membuat metode pencegahan kehilangan data, perlindungan integritas data, metode otentikasi dan otorisasi. Setiap vendor dan perusahaan harus menggunakan algoritma kriptografi yang memiliki standar seperti NIST untuk pengamanan data di cloud. Hal ini juga berguna untuk melakukan evaluasi ulang terhadap algoritma dan kunci yang digunakan untuk memastikan kekuatan proteksi setiap tahun nya. Konsumen yang yang menggunakan teknologi cloud computing harus memahami kontrol keamanan yang terkait dengan data di lingkungan cloud computing yang memiliki penyewa yang banyak. Modul Keamanan menggunakan perangkat keras sangat direkomendasikan untuk menyimpan kunci.

DOI: https://doi.org/10.29103/techsi.v11i1.1357

b. Penggunaan Administrative Privileges

Sebuah organisasi pengguna cloud computing harus meminimalkan penggunaan Administrative Privileges dalam operasional sehari hari, dan hanya menggunakan akun administratif pada saat dibutuhkan saja. Sistem yang otomatis sangat harus digunakan untuk menginventarisasi semua akun administratif dan memvalidasi setiap pengguna yang memiliki hak administratif di laptop, desktop, dan server yang diberi wewenang oleh pimpinan. Semua password administratif harus rumit termasuk angka, huruf dan karakter khusus yang tercampur, tanpa adanya kata-kata dalam kamus untuk password. Semua kata kunci default untuk sistem operasi, aplikasi, firewall, router, titik akses nirkabel, dan sistem lainnya harus diubah sebelum menerapkan perangkat baru dalam sistem jaringan. Password akun layanan juga harus panjang, sulit ditebak, dan selalu berubah secara reguler. Password yang tersimpan harus dienkripsi atau di hash. Password yang di hash harus mengikuti panduan yang diberikan di standard security seperti NIST SP 800-132 atau panduan serupa.

Log akses harus digunakan untuk memastikan bahwa akun administratif hanya akan digunakan untuk aktivitas administrasi sistem. Administrator harus menggunakan kata kunci yang unik dan berbeda untuk akun administratif dan non-administratif mereka. Administrator harus di edukasi dengan baik tentang keamanan data. Sistem operasi harus dikonfigurasi sedemikian rupa sehingga password harus ditukar secara reguler, minimal dalam enam bulan ke sekali. Sistem harus membatasi jumlah percobaan login masuk yang gagal ke akun administrator. Otentikasi multifaktor harus digunakan untuk semua akses administratif, serta akses administratif domain. Jenis otentikasi ini bisa mencakup metode yang berbeda, seperti menggunakan kartu pintar dengan sertifikat, biometrik, token One Time Password (OTP) dan lain lain. Bila mengaktifkan otentikasi berbasis sertifikat multifaktor, kunci privat harus dilindungi dengan menggunakan kata kunci yang kuat atau disimpan dengan aman dan terpercaya. Token perangkat keras Administrator harus diminta untuk mengakses sistem dengan menggunakan akun non-administratif dan log harus terinstal sepenuhnya.

DOI: https://doi.org/10.29103/techsi.v11i1.1357

c. Kontrol Akses Nirkabel dari Data

Perusahaan atau organisasi yang menggunakan cloud computing dan memiliki jaringan nirkabel harus menggunakan perangkat nirkabel komersial untuk scanning, deteksi dan juga harus menggunkan sistem deteksi intrusi nirkabel komersial. Administrator keamanan harus secara teratur memonitor lalu lintas data pada jaringan nirkabel dengan menggunakan network monitor. Untuk mengetahui apakah lalu lintas data pada jaringan nirkabel sudah menggunakan enkripsi yang disetujui atau protokol keamanan yang kuat. Dalam konteks ini, admin keamanan juga harus menggunakan perangkat manajemen jarak jauh pada bagian jaringan kabel untuk mengetahui tentang potensi dan perangkat nirkabel yang terhubung ke sistem yang dikelola.

d. Recovery Data di Cloud Computing

Sangat penting setiap sistem yang menggunakan cloud computing harus memiliki prosedur back up otomatis setidaknya seminggu sekali, dan untuk sistem yang menyimpan informasi sensitif lebih sering dari pada sekali dalam seminggu. Prosedur backup keseluruhan bahkan harus mencakup sistem operasi, aplikasi dan data yang ada. Sistem backup yang diterapkan pada cloud computing sebaiknya lebih dari satu. Selain dari pada itu, sekali per kuartal, perlu dilakukan evaluasi terhadap sampel acak dari sistem backup dengan mencoba merecovery-nya di lingkungan uji coba. Sistem yang direcovery, harus dipastikan bisa menjamin keutuhan sistem operasi, aplikasi dan data dari backup menyeluruh. Sehingga, jika ada infeksi malware, prosedur restore bisa menggunakan versi backup terakhir sebelum terjadi infeksi.

e. Batas Pertahanan Data di Cloud

Pertahanan sistem imformasi dalam satu organisasi atau perusahaan yang menggunakan cloud computing dapat diimplementasikan dengan menggunakan IDS (Instrution Detection System) dan sniffers untuk mendeteksi serangan dari sumber eksternal ke sistem internal DMZ (Demillitary Zone) organisasi dan juga sebaliknya. Hal ini juga bermanfaat untuk menolak komunikasi dengan alamat IP berbahaya yang sudah

DOI: https://doi.org/10.29103/techsi.v11i1.1357

diketahui dan bisa juga membatasi akses hanya ke situs terpercaya saja. Organisasi atau perusahaan tersebut harus menggunakan perangkat IPS berbasis jaringan sebagai tambahan IDS untuk memblokir akibat buruk dari serangan. Otentikasi dua faktor sangat diperlukan saat menggunakan akses masuk jarak jauh melalui VPN. Selain dari pada itu, hanya sistem DMZ yang boleh berkomunikasi dengan sistem jaringan internal organisasi melalui proxy atau firewall melalui saluran resmi. Sehingga, aktivitas yang mencurigakan dapat dengan mudah dideteksi dengan menggunakan analisis NetFlow pada jaringan DMZ.

5. Kesimpulan

Tujuan utama dari penelitian ini adalah untuk menganalisis dan mengevaluasi metode-metode pengamanan untuk perlindungan data untuk cloud computing. Penelitian ini mengevaluasi metode pengamanan yang terpenting untuk perlindungan data yang digunakan oleh penyedia-penyedia layanan cloud computing. Mekanisme pengamanan ini diklasifikasikan dalam empat kategori yaitu: metode otentikasi, kerahasiaan dan privasi, kontrol akses dan otorisasi. Penelitian ini bermaksud menjawab sebuah keraguan dari pihak penguna layanan cloud computing, bisakah layanan cloud computing diandalkan dalam hal pengamanan dan perlindungan data pengguna. Perlindungan data pengguna pada layanan cloud computing ini bisa di maksimalkan jika semua langkah yang direkomendasikan dijalankan. Rekomendasi yang diberikan yaitu untuk menjalankan metode otentikasi, meningkatkan kerahasiaan dan privasi, metode kontrol akses dan otorisasi yang memadai, maka cloud computing akan dapat dipercaya dalam hal perlindungan data. Penulis juga menyarankan beberapa hal yang harus dipertimbangkan untuk pengamanan data yang lebih baik dalam cloud computing, seperti penggunaan hak administratif yang tepat, kontrol akses nirkabel data dalam sistem yang menggunakan jaringan nirkabel, recovery data dan peningkatan batas pertahanan pada cloud computing.

DOI: https://doi.org/10.29103/techsi.v11i1.1357

Daftar Pustaka

[1] Badger L., Grance, Patt-Corner R. and Voas J., (2011). "Cloud computing synopsis and recommendations (draft), nist special publication 800-146", Recommendations of the National Institute of Standards and Technology, Tech. Rep.

[2] Chouhan P., Singh R., (2016), "Security Attacks on Cloud Computing With Possible Solution"., International Journal of Advanced Research in Computer Science and Software Engineering 6(1), pp.

[3] Khalid U, Ghafoor A., Irum M., and Shibli M. A., (2013), "Cloud based secure and privacy enhanced authentication & authorization protocol", Procedia Computer Science, 22, 680-688.

[4] T. Acar, M. Belenkiy and A. Küpçü, (2013) "Single password authentication", Computer Networks, 57(13), 2597-2614.

[5] Singh, N. & Singh, A.K. (2018) "Data Privacy Protection Mechanism" Data Sci. Eng. 3: 24. https://doi.org/10.1007/s41019-017-0046-

[6] Wang G., Liu Q., Wu J. and Guo M., (2011). "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, 30(5), 320-331.

[7] Fan C. I., and Huang S. Y., (2013). "Controllable privacy preserving search based on symmetric predicate encryption in cloud storage", Future Generation Computer Systems, 29(7), 1716-1724.

[8] Rizzo C., (2019) "Integrated Design ensures availability and protection of critical sensitive data with Online Tech's cloud infrastructure". Access 20 april 2019, from:

https://www.businesswire.com/news/home/20190123005046/en

[9] Younis A. Younis, Kifayat K., Merabti M., (2014). "An Access Control Model for Cloud Computing". Journal of Information Security and Applications, Volume 19, Issue 1, February 2014, Pages 45-6

[10] CA Technology. (2014)., "Expanding Web Single Sign on to Cloud and Mobile Environment"., https://www.ca.com/content/dam/ca/us/files/ebook/expanding-web-sso-to-cloud-and-mobile-environments.pdf

[11] Cigoj, Primož & Jerman, Borka. (2015). An Authentication and Authorization Solution for a Multiplatform Cloud Environment. Information Security Journal: A Global Perspective. 24. 1-11. 10.1080/19393555.2015.1078424.

[12] Chadwick D. W., and Fatema K., (2012) "A privacy preserving authorisation system for the cloud", Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.

[13] Hange M., (2011) "Security Recommendations for Cloud Computing Providers", Federal Office for Information Security

[14] Brunette G., and Mogull R., (2009) "Security guidance for critical areas of focus in cloud computing v2", Cloud Security Alliance, 1-76.

DOI: https://doi.org/10.29103/techsi.v11i1.1357