IMPLEMENTASI PROTEKSI *CLIENT-SIDE* PADA *PRIVATE CLOUD STORAGE NEXTCLOUD*

Dedy Hariyadi[1], Imam Puji Santoso[2], Ramadhana Saputra[3]

[1] Teknologi Informasi, Universitas Jenderal Achmad Yani Yogykarta
[1,2] Teknik Informatika, Universitas Jenderal Achmad Yani Yogykarta
Jl. Siliwangi, Ringroad Barat, Banyuraden, Gamping, Sleman
Daerah Istimewa Yogyakarta
[1] milisdad@gmail.com, [2] adjiesan09@gmail.com, [3] *ramadhanasaputra45@gmail.com*

Abstract

At present almost every device is connected with cloud computing technology. Cloud computing technology that offers attractive services is Cloud Storage such as Google Drive, Dropbox, One Drive, Mega, and others. Such cloud storage technology can be applied in a private environment or on-premise. Cloud Storage software that can be installed in a private environment such as OwnCloud, Nextcloud, SeaFile, and others. The implementation of Cloud Storage needs to be watched out because it has a security gap when transmitting data from the client to the server or vice versa and the protection of files stored on the Cloud Storage server. In this study shows the results of testing the vulnerability of storing files and directories in Cloud Storage providers as well as providing solutions to overcome these security.

Keywords : *Cloud Storage, Cloud Computing, Encryption, Information Security*

Abstrak

Saat ini hampir setiap perangkat terhubung dengan teknologi komputasi awan. Teknologi komputasi awan yang menawarkan layanan menarik adalah *Cloud Storage* seperti Google Drive, Dropbox, One Drive, Mega, dan lain-lain. Teknologi *Cloud Storage* semacam itu dapat diterapkan di lingkungan *private* atau *on-premise*. Peranti lunak *Cloud Storage* yang dapat diinstall di lingkungan *private* diantaranya, OwnCloud, Nextcloud, SeaFile, dan lain-lain. Implementasi Cloud Storage perlu diwaspadai karena memiliki celah keamanan saat transmisi data dari *client* ke server atau sebaliknya dan tidak terproteksinya berkas yang tersimpan pada *Cloud Storage* server. Pada penelitian ini menunjukkan hasil pengujian kerentanan menyimpan berkas dan direktori di penyedia *Cloud Storage* berserta memberikan solusi mengatasi keamanan tersebut.

Kata kunci : *Cloud Storage, Cloud Computing,* Enkripsi, Keamanan Informasi

1. Pendahuluan

Menurut *National Institute of Standards and Technology, US Department of Commerce* komputasi awan memiliki karakteristik diantaranya pengguna dapat mengelola layanan secara mandiri *(on-demand self-service)*, dapat diakses melalui jaringan atau pun *platform* apa pun *(broad network access)*, mengumpulkan dan mengelola sumber daya komputasi *(resource pooling)*, memudahkan dalam pengelolaan yang menyesuaikan dengan kebutuhan secara cepat (*rapid elasticity*), dan terdapat sistem pengukuran pada jenis layanan (*measured service*) (Mell & Grance, 2011). Karakteristik tersebut mempengaruhi kesiapan infrastruktur dalam implementasi teknologi komputasi awan, oleh

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)

sebab itu harus dilakukan pertimbangan terhadap kebutuhan masing-masing organisasi / instansi / perusahaan. Bandwidth internet merupakan salah satu hal yang perlu dipertimbangkan untuk mengakses layanan teknologi komputasi awan yang stabil (Ashari & Setiawan, 2011). *Cloud Storage* merupakan contoh layanan komputasi yang dapat diterapkan di lingkungan *private* atau *on-premise* untuk mengatasi permasalahan keterbatasan bandwidth internet.

Selain memiliki keterbatasan bandwidth internet, implementasi *Cloud Storage* pada pihak ketiga memiliki keterbatasan kapasitas. Solusi untuk menangani hal ini dapat diterapkan melakukan gabungan antara penyedia komputasi awan (pihak ketiga) dan implementasi di lingkungan *private*. Kelebihannya menggunakan model semacam ini kapasitas lebih besar, data lebih mudah terkelola dan tidak ada keterbatasan akses bandwidth internet (Surosa, Fitri, & Nathasia, 2018).

Technische Universität Berlin telah menerapkan *Cloud Storage* yang dapat diakses di lingkungan universitas menggunakan *OwnCloud* dengan jumlah pengakses 40.000 mahasiswa (Hildmann & Kao, 2014). Sekolah Tinggi Ilmu Kesehatan Aisyiyah Yogyakarta (sekarang Universitas Aisyiyah Yogyakarta) melakukan pengembangan *Cloud Storage* yang diperuntukan untuk karyawan menggunakan *OwnCloud* diatas FreeNAS (Purnomo & Sugiantoro, 2015). Pada lingkungan pemerintah juga telah menerapkan teknologi *Cloud Storage* secara *on-promise*, diantaranya Kementerian Perindustrian mengunakan Nextcloud (Nurohman, H, & Riana, 2018).

Walaupun implementasi *Cloud Storage* di lingkungan terpercaya, sebaiknya komunikasi datanya harus diamankan. Untuk melindungi data yang ditransmisikan pada layanan *Cloud Storage* perlu menerapkan sistem keamanan berbasis *SSL (Secure Socket Layer)* (Khaliq, 2014). Pada saat transmisi data antara *client* dengan *Cloud Storage server* dapat juga diamankan secara selektif menggunakan IPTables dan VPN (Hariyadi & Azhar, 2017).

2. Kajian Pustaka

2.1. Definisi Komputasi Awan

Department of Commerce Amerika Serikat melalui National Institute of Standards and Technology (NIST) mengeluarkan rekomendasi teknologi komputasi awan. Pada rekomendasi tersebut didefinisikan teknologi komputasi awan memiliki karakter yang esensial (Mell & Grance, 2011):

1. *On-demand self-service*, pengguna dapat secara mandiri tanpa menghubungi penyedia layanan untuk mengelola sumber daya komputasi.
2. *Broad network access*, layanan tersedia pada jaringan yang dapat diakses dari mana saja.
3. *Resource pooling*, sumber daya komputasi terkumpul pada suatu sistem yang mempermudah dalam melayani pengguna tanpa ketergantungan lokasi.
4. *Rapid elasticity*, mendukung proses otomatisasi dan elastis dalam pengelolaan sumber daya komputasi.
5. *Measured service*, transparasi dalam pengukuran sumber daya komputasi yang dikelola sehingga memudahkan pengendalian dan pelaporan.

2.2. Ekosistem Komputasi Awan

Model ekosistem teknologi komputasi awan dapat dibagi menjadi tiga (Karie, Venter, & Kabarak, 2013):

1. *Public Cloud*, ekosistem komputasi awan yang tersedia secara publik melalui internet. Layanan public cloud yang diberikan diantaranya infrastruktur, platform, aplikasi, dan lain-lain.
2. *Private Cloud*, ekosistem komputasi awan yang keseluruhan sumber daya komputasinya diimplementasi pada suatu institusi.
3. *Community Cloud*, ekosistem komputasi awan dengan sumber daya komputasinya tersedia untuk melayani suatu komunitas atau grup tertentu.

Ketiga model ekosistem teknologi komputasi awan tersebut di Indonesia telah diimpelementasi di berbagai perusahaan, institusi pemerintah, organisasi nirlaba, dan sebagainya. Berbagai *smart system* yang diterapkan pada pemerintah juga telah menerapakan teknologi komputasi awan baik *private cloud* dan *community cloud* dalam bentuk smart city (Djunaedi et al., 2018).

Penelitian sebelumnya teknologi komputasi awan digunakan untuk media pembelajaran Keamanan Informasi di *Hellenic Air Force Academy*, Yunani. Materi yang dipelajari pada sistem berbasis komputasi diantaranya: *Windows Forensics, Network Forensics, Linux Forensics, Android Forensics, Web Application Security, Malware Analysis, Code Reversing, Cryptography,* dan *Steganography* (Andreatos, 2017). Namun, pada penelitian tersebut belum membahas tentang proteksi berkas pada teknologi komputasi awan. Oleh sebab itu pada penelitian ini akan melakukan evaluasi proteksi berkas yang terimplementasi pada teknologi komputasi awan.

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)

2.3. Proteksi Data *Cloud Storage*

Transmisi data pada *Cloud Storage* yang menggunakan protokol HTTP sangat rentan dilakukan penyadapan sehingga peretas dapat mencuri informasi (Chordiya, Majumder, & Javaid, 2018). Oleh sebab sistem *Cloud Storage* memerlukan proteksi, adapun metodenya sebagai berikut (Bernd Gastermann, Stopper, Kossik, & Katalinic, 2014):

1. Proteksi *Server-side*, proses proteksi terjadi di sisi *server* yang memanfaatkan sistem proteksi pada sistem operasi, misal MS Windows menggunakan BitLocker atau Ubuntu menggunakan eCryptfs *(Enterprise-class Cryptographic Filesystem)*.
2. Transmisi Terenkripsi, melakukan proses proteksi pada protokol yang digunakan misal protokol web maka akan menggunakan protokol HTTPS.
3. Proteksi *Client-side*, proses proteksi pada sisi klien yang memanfaatkan enkripsi pada *virtual drive*.

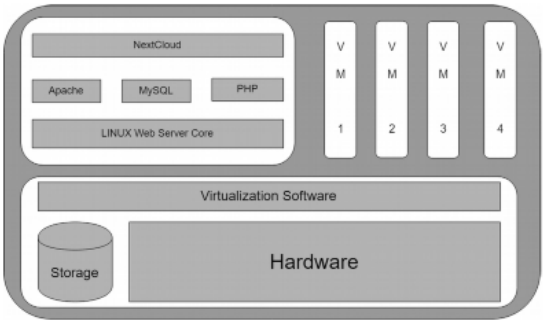
Implementasi teknologi komputasi awan memiliki beberapa tantangan terkait dengan ancaman keamanan. Adapun ancaman terhadap infrastruktur komputasi diantaranya (Kumar, Meena, Singh, & Vardhan, 2016):

1. *Threat to Data Confidentiality*, kerahasiaan data harus dapat dideteksi dari penyerang baik dari luar sistem maupun internal.
2. *Threat to Data Integrity*, ancaman integritas suatu data harus terdeteksi baik pengubahan atau hilangnya data oleh pihak yang tidak berhak.
3. *Threat to Data Availability*, munculnya ancaman terkait kesulitan pengguna layanan komputasi terkait data yang disimpan.

Untuk menjaga dari tiga ancaman tersebut maka pada penelitian ini menerapkan proteksi pada client-side.

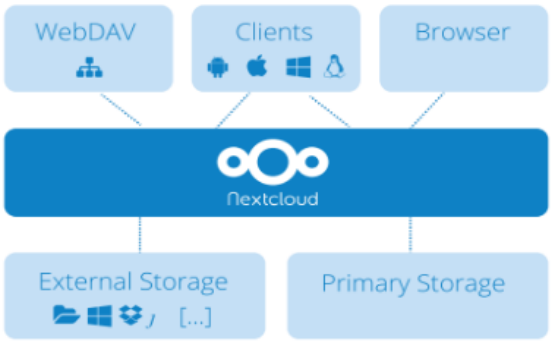
2.4. Arsitektur Cloud Storage Server

Pada penelitian ini mengadopsi arsitektur implementasi *Cloud Storage* yang diterapkan pada Usaha Mikro, Kecil dan Menengah di Austria. Arsitektur *Cloud Storage* yang menggunakan peranti lunak *Nextcloud* terpasang diatas sebuah sistem operasi yang berjalan pada mesin virtual. Sehingga *Nextcloud* yang menggunakan PHP, MySQL dan Apache tidak mengganggu gugusan mesin virtual lain dengan teknologi serupa (B Gastermann, Stopper, Kossik, & Katalinic, 2015). Gambar 1 menunjukan arsitektur *Cloud Storage server* menggunakan Nextcloud yang diterapkan pada penelitian ini.



Gambar 1. Arsitektur Cloud Storage Nextcloud

Nextcloud merupakan perangkat lunak buatan perusahaan Nextcloud GmbH yang diterapkan pada teknologi komputasi awan. Nexcloud menyediakan lapisan untuk mengakses suatus berkas secara umum namun masih menjaga mekanisme manajemen pengendalian oleh pengelola Teknologi Informasi dan Komunikasi pada suatu organisasi sebagai wujud manajemen risiko. Bentuknya penyimpanan data berbasis public cloud, Windows network drive ataupun penyimpanan lokal dapat dikelola, diamankan dan dikendalika melalui proses pada sistem Nextcloud. Gambar 2 menunjukan sistem layanan penyimpanan berkas terpadu yang terdapat pada Nextcloud (Karlitschek & Mache, 2017)



Gambar 2. Layanan Penyimpanan Terpadu Nextcloud.

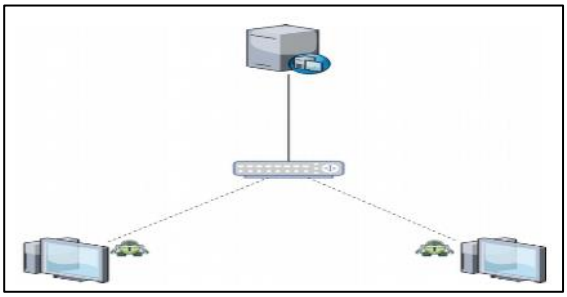
2 Metode Penelitian

Berdasarkan Gambar 1 *Nextcloud* terinstall pada mesin virtual dengan sistem operasi berkernel Linux. Pada server hanya terinstall Nextcloud tanpa menerapkan proteksi pada *file system*. Proteksi diterapkan pada sisi *client* menggunakan peranti lunak Cryptomator. Peranti lunak Cryptomator merupakan produk dari

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)

perusahaan rintisan asal Bonn, Jerman yang berfungsi memproteksi data di layanan *Cloud Storage* berbasis proteksi *client-side* sehingga dapat melindungi data seperti foto, data penting perusahaan, informasi perbankan atau data penting lainnya (Cryptomator, 2017).

Cryptomator akan terinstall pada klien yang dapat mengakses Nextcloud server. Implementasi Nextcloud server dan client yang terinstall Cryptomator pada jaringan internal suatu organisasi. Adapun topologi implementasi Cryptomator pada penelitian ini dapat dilihat pada Gambar 3.



Gambar 3. Topologi Implementasi Cryptomator

3 Hasil dan Pembahasan

Pada penelitian ini sistem operasi yang terinstall pada server terbagi menjadi dua bagian, yaitu *Host Operating System* dan G*uest Operating System (Mahjoub, Mdhaffar, Ben Halima, & Jmaiel, 2011)*. *Host Operating System* yang digunakan adalah Linux Mint[1] versi 19.1 yang terinstall perangkat lunak virtualisasi, VirtualBox[2]. *Guest Operating System* menggunakan Ubuntu Server versi 18.04[3] yang terinstall diatas VirtualBox sebagai mesin virtual.

Guest Operating System terinstall LAMP (Linux-Apache-MySQL-PHP) yang merupakan paket bawaan dari Ubuntu Server versi 18.04. Setelah komponen dari LAMP telah terinstall maka dilanjutkan install Nextcloud, sesuai dengan Gambar 1.

Pengujian dilakukan dengan melakukan installasi Cryptomator pada sisi *client*. Pada penelitian ini *client* yang digunakan menggunakan sistem operasi berkernel Linux, Linux Mint versi 19.1. Sebelum Cryptomator terinstall, aplikasi client dari *Nextcloud* harus terinstall terlebih dahulu. Hal ini juga berlaku untuk layanan *Cloud Storage* lainnya supaya terdefinisi direktori berserta berkas-berkas didalam direktori tersinkron dengan *Cloud Storage server*.

Setelah Nextcloud *Client* terinstall maka aplikasi Cryptomator menentukan ruang brangkas atau *vault* untuk meletakan berkas maupun direktori yang akan diproteksi. Berkas atau direktori yang diproteksi menggunakan Cryptomator tidak mudah dibaca oleh oleh pihak manapun termasuk Administrator dari penyedia layanan *Cloud Storage*. Gambar 4 menunjukan berkas atau direktori yang dapat dilihat oleh pihak penyedia *Cloud Storage*. Sedangkan Gambar 5 menunjukan berkas atau direktori yang dapat dilihat oleh pihak penyedia *Cloud Storage* dalam bentuk nama berkas atau direktori yang terproteksi.

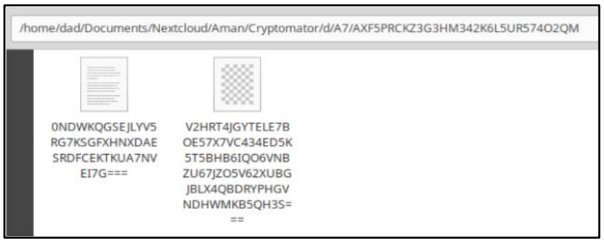
1. https://www.linuxmint.com/
2. https://www.virtualbox.org
3. https://ubuntu.com/

```
root@NextCloud:/var/www/html/nextcloud/data/unjani/files# ls -l
total 5052
drwxr-xr-x 3 www-data www-data    4096 Feb 19 10:49  Aman
drwxr-xr-x 2 www-data www-data    4096 Feb  2 23:37  Documents
-rw-r--r-- 1 www-data www-data 4646274 Feb  2 23:37 'Nextcloud Manual.pdf'
-rw-r--r-- 1 www-data www-data  462413 Feb  2 23:37  Nextcloud.mp4
-rw-r--r-- 1 www-data www-data   37042 Feb  2 23:37  Nextcloud.png
drwxr-xr-x 2 www-data www-data    4096 Feb  2 23:37  Photos
drwxr-xr-x 4 www-data www-data    4096 Feb  3 00:22  Proteksi
drwxr-xr-x 2 www-data www-data    4096 Feb  2 23:50  Testing
```

Gambar 4. Berkas dan Direktori yang Tersimpan di Nextcloud

```
root@NextCloud:/var/www/html/nextcloud/data/unjani/files/Aman/Cryptomator/d# ls -l
total 8
drwxr-xr-x 3 www-data www-data 4096 Feb 19 10:49 A7
drwxr-xr-x 3 www-data www-data 4096 Feb 19 10:49 UK
root@NextCloud:/var/www/html/nextcloud/data/unjani/files/Aman/Cryptomator/d# ls A7/AXF5PRCKZ3G3HM342K6L5UR574O2QM/
'0NDWKQGSEJLYV5RG7KSGFXHNXDAESRDFCEKTKUA7NVEI7G===' 'V2HRT4JGYTELE7BOE57X7VC434ED5K5T5BHB6IQO6VNBZU67JZO5V62XUBGJBLX4QBDRYPHGVNDHWMKB5QH3S=='
root@NextCloud:/var/www/html/nextcloud/data/unjani/files/Aman/Cryptomator/d# ls UK/XFA3M3SOCH7OELAUD5ACAHBBT2UDCS/
root@NextCloud:/var/www/html/nextcloud/data/unjani/files/Aman/Cryptomator/d#
```

Gambar 5. Berkas dan Direktori yang Terproteksi di Nextcloud



Gambar 6. Proteksi Cryptomator pada Sisi Client

pada sisi *client* juga tampak teracak nama berkas dan direktori jika dilhat tanpa menggunakan aplikasi Cryptomator, lihat Gambar 6. Sedangkan berkas yang dapat dilihat dan diakses dengan mudah jika telah mengaktifkan

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)

dan membuka kunci ruang berkas Cryptomator, lihat Gambar 7.

Gambar 7. Virtual Drive dengan Proteksi Terbuka

Kesimpulan

Tidak semua penyedia layanan *Cloud Storage* memberikan jaminan proteksi enkripsi pada sistem penyimpanan berkas dan direktori. Sebaiknya setiap memanfaatkan layanan *Cloud Storage* membaca syarat dan ketentuan yang berlaku pada penyedia. Berdasarkan hasil pengujian terbukti bahwa penyedia layanan *Cloud Computing* yang tidak memberikan jaminan keamanan berupa enkripsi pada berkas yang tersimpan pada server maka pihak Administrator dapat melihat dan membuka dengan mudah. Solusi mengantisipasi Administrator dari pihak penyedia layanan *Cloud Storage* yang tidak beretika maka dari sisi *client* atau pengguna dapat menerapkan proteksi *Client-side* menggunakan Cryptomator. Peranti lunak Cryptomator tidak hanya digunakan untuk proteksi berkas dan direktori di lingkungan komputasi awan saja. Namun, aplikasi Crytopmator dapat diimplementasikan pada lingkungan atau media penyimpan lokal.

Daftar Pustaka

[1] Andreatos, A. S. (2017). Designing Educational Scenario to Teach Network Security. *2017 IEEE Global Engineering Education Conference (EDUCON)*.

[2] Ashari, A., & Setiawan, H. (2011). Cloud Computing: Solusi ICT. *Jurnal Sistem Informasi*, *3*(2), 80. https://doi.org/10.16192/j.cnki.1003-2053.2015.02.013

[]. Chordiya, A. R., Majumder, S., & Javaid, A. Y. (2018). Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools. *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 438–443. https://doi.org/10.1109/EIT.2018.8500144

[4] Cryptomator. (2017). *Make Your Cloud Great Again – Cloud Encryption with Cryptomator*.

[5] Djunaedi, A., Permadi, D., Nugroho, L. E., Widyawan, Rachmawati, R., Hidayat, A., … Egavaranda, S. (2018). *Membangun Kota dan Kabupaten Cerdas: Sebuah Panduan bagi Pemerintah Daerah*. (Tim CFDS, Ed.) (Pertama). Yogyakarta: Gadjah Mada University Press.

[6]. Gastermann, B, Stopper, M., Kossik, A., & Katalinic, B. (2015). On-premises cloud storage - Security aspects for small and medium-sized enterprises. In *The International MultiConference of Engineers and Computer Scientists* (Vol. 2, hal. 931–937). Diambil dari https://www.scopus.com/inward/record.uri?eid=2-s2.0-84937848841&partnerID=40&md5=e4c65b78a9312763880cd18f2f64d271

[7] Gastermann, Bernd, Stopper, M., Kossik, A., & Katalinic, B. (2014). Secure Implementation of an On-premises Cloud Storage Service for Small and Medium-sized Enterprises. *Procedia Engineering*, *100*, 574–583. https://doi.org/10.1016/j.proeng.2015.01.407

[8] Hariyadi, I. P., & Azhar, R. (2017). Pengamanan Layanan Private Cloud Storage Menggunakan HTTPS, IPTables dan SSTP. In *Seminar Nasional TIK dan Ilmu Sosial*.

[9] Hildmann, T., & Kao, O. (2014). Deploying and extending on-premise cloud storage based on ownCloud. In *International Conference on Distributed Computing Systems* (Vol. 30-June-20, hal. 76–81). https://doi.org/10.1109/ICDCSW.2014.18

[9] Venter, H. S., & Kabarak, K. (2013). An Ontological Framework for a Cloud Forensic Environment. In *Proceedings of the European Information Security Multi-Conference* (hal. 112–122). Diambil dari http://41.89.99.18:8080/bitstream/handle/123456789/274/Nickson Karie 1.pdf?sequence=1&isAllowed=y

[10]. Karlitschek, F., & Mache, N. (2017). *Nextcloud Solution Architecture Bring data back under control of IT Overview of the Nextcloud Architecture*.

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)

[11]. Khaliq, I. (2014). Implementasi Cloud Computing Dengan Keamanan SSL (Secure Socket Layer). *Jurnal Ilmiah OnLine STMIK – Politeknik PalComTech*, 1–13.

[12]. Kumar, M., Meena, J., Singh, R., & Vardhan, M. (2016). Data outsourcing: A threat to confidentiality, integrity, and availability. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1496–1501. https://doi.org/10.1109/ICGCIoT.2015.7380703

[13]. Mahjoub, M., Mdhaffar, A., Ben Halima, R., & Jmaiel, M. (2011). A comparative study of the current cloud computing technologies and offers. *Proceedings - 2011 1st International Symposium on Network Cloud Computing and Applications, NCCA 2011*, 131–134. https://doi.org/10.1109/NCCA.2011.28

[14].Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. *Recommendations of the National Institute of Standards and Technology 800-145*. Diambil dari http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[15]. Nurohman, M., H, A. S., & Riana, E. (2018). Perancangan Private Cloud Computing pada Kementerian Perindustriuan Jakarta. *Jurnal Teknik Komputer*, *4*(1), 48–55.

[16]. Purnomo, A., & Sugiantoro, B. (2015). *Pengembangan Cloud Storage dengan Pemanfaatan Virtualisasi Server pada Sistem Operasi Network Attached Storage (FreeNAS)*. Universitas Islam Negeri Sunan Kalijaga.

[17]. Surosa, S. A. N., Fitri, I., & Nathasia, N. D. (2018). Rancang Bangun Hybrid Cloud Storage Berbasis Infrastucture As A Service (IAAS). *Informatika Merdeka Pasuruan*, *3*(2), 54–60.

[18] W. (STMIK L. Lalu Supriadi Kalaena, Bagye, "Implementasi Network Attached Storage (NAS) Menggunakan Freenas Pada Stmik Lombok," *J. Manaj. Inform. dan Sist. Inf.*, vol. 1, no. 1, pp. 6–10, 2018.

ISSN : 2614-1701 (Cetak) – 2614-3739 (Online)