PENGEMBANGAN SISTEM KEAMANAN PUSAT DATA DENGAN MEMANFAATKAN GROUP POLICY MANAGEMENT

Herlina Harahap[1], Divi Handoko[2]

[12]Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan

e-mail: [1]herlinaharahap@unhar.ac.id, [2]divihandoko@unhar.ac.id

ABSTRAK

Semakin meningkatnya perkembangan komunikasi data membuat semakin pentingnya aspek keamanan dan kerahasiaan data. Teknologi informasi yang berkembang sangat pesat di dalam kehidupan manusia saat ini, membuat kebutuhan akan sistem penyimpanan data terpusat menjadi sesuatu yang penting dalam menyimpan arsip dan dokumen digital. Seiring dengan kemajuan tersebut kebutuhan akan keamanan pada media penyimpanan sangat diperlukan karena kemajuan teknologi berbanding lurus dengan kejahatan-kejahatan yang ada dalam internet itu sendiri. Maka dari itu bagaimana membangun sistem kemanan Pusat Data pada jaringan LAN menggunakan Group Policy Management pada Windows Server 2012 dengan tujuan memberikan kemanan Pusat Data pada tindakan user dalam memindahkan data dari komputer client ke tempat penyimpanan lain. Dengan membangun sistem tersebut, pengguna nantinya dapat mencegah pencurian data yang terdapat pada komputer clinet. Untuk melakukan pengamanan data, diperlukan adanya alat bantu yang dapat digunakan untuk mengatur keamanan dan beberapa kebijakan lainnya di dalam program Microsoft windows. Dengan adanya Active Directory dan Group Policy Management pada Window Server 2012 menyediakan cara yang mudah dan efektif untuk mengelola preferensi dan pengaturan untuk komputer dan pengguna. Group Policy Management menyediakan cara yang sangat sederhana untuk melihat apa yang terjadi dalam satu Group Policy Object (GPO) tertentu. Berdasarkan pengujian dapat disimpulkan yaitu dengan adanya Group Policy Management dapat meningkatkan sistem keamanan data sehingga data tersebut tidak dapat di copy atau diduplikat dan disimpan ditempat media penyimpanan yang lain.

Kata kunci: Keamanan Data, *Windows Server 2012, Active Directory, Group Policy Management*.

ABSTRACT

The increasing development of data communications makes the aspect of data security and confidentiality increasingly important. Information technology is developing very rapidly in human life today, making the need for a centralized data storage system important for storing digital archives and documents. Along with this progress, the need for security on storage media is very necessary because technological progress is directly proportional to the crimes that exist on the internet itself. Therefore, how to build a Data Center security system on a LAN network using Group Policy Management on Windows Server 2012 with the aim of providing Data Center security based on user actions in moving data from client computers to other storage locations. By building this system, users will be able to prevent theft of data on clinet computers. To secure data, it is necessary to have tools that can be used to manage security and several other policies in the Microsoft Windows program. With Active Directory and Group Policy Management in

Window Server 2012 it provides an easy and effective way to manage preferences and settings for computers and users. Group Policy Management provides a very simple way to see what's happening within a particular Group Policy Object (GPO). Based on the testing, it can be concluded that the existence of Group Policy Management can improve the data security system so that the data cannot be copied or duplicated and stored in other storage media.

Keywords: *Data Security, Windows Server 2012, Active Directory, Group Policy Management*

1. PENDAHULUAN

Semakin meningkatnya perkembangan komunikasi data membuat semakin pentingnya aspek keamanan dan kerahasiaan data. Teknologi informasi yang berkembang sangat pesat didalam kehidupan manusia saat ini, membuat kebutuhan akan sistem penyimpanan data terpusat menjadi sesuatu yang penting dalam menyimpan arsip dan dokumen digital. Data tidak hanya disimpan dalam PC desktop atau media penyimpanan saja tetapi media penyimpanan data terpusat menjadi alternative dalam media penyimpanan, guna menjaga dari kehilangan data atau backup data. Seiring dengan kemajuan tersebut kebutuhan akan keamanan pada media penyimpanan sangat diperlukan karena kemajuan teknologi berbanding lurus dengan kejahatan-kejahatan yang ada dalam internet itu sendiri. Dengan adanya kejahatan internet ini para pemakai semakin tidak aman dan menjadi intaian para penjahat setiap kali ber-internet, maka diperlukan solusi agar data yang disimpan pada media penyimpanan bisa aman sesuai keinginan.

Pada penelitian yang terkait sebelumnya dengan topik pembahasan mengenai Analisis Penerapan Sistem Keamanan Fisik Pada Data Center Untuk Melindungi Data Organisasi yang dilakukan oleh Digky Bima Priatmoko, dkk dari Universitas Brawijaya Malang. Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI) IKIP PGRI MADIUN. Tujuan dalam penelitian ini yaitu mendeskripsikan penerapan Sistem Keamanan Fisik pada data center PMBSI IKIP PGRI Madiun dan menganalisis apakah penerapan Sistem Keamanan Fisik pada data center mampu melindungi data organisasi milik PMBSI IKIP PGRI Madiun. (Priatmoko dkk, 2016). Dan dengan topik pembahasan mengenai Implementasi Pembatasan Akses Pemakai Komputer Menggunakan Group Policy Object Di Windows Server 2012 R2 yang dilakukan oleh Marliana Sari dari Politeknik Negeri Medan. Didalam penelitian tersebut memaparkan implementasi keamanan jaringan menggunakan Group Policy Object. Active Directory bertindak sebagai otoritas terpusat terhadap keamanan jaringan, melakukan verifikasi terhadap akses user, dan yang paling penting yaitu sebagai titik integrasi untuk membuat sistem bisa bekerja secara sinergis dalam mengkonsolidasi tugas-tugas manajemen. (Sari, 2017)

Pengamanan data kini telah menjadi kebutuhan organisasi manapun. Ancaman keamanan meningkat dari hari ke hari dan membuat jaringan kabel/nirkabel berkecepatan tinggi dan layanan internet, tidak aman dan tidak dapat diandalkan. Pusat

data adalah fasilitas yang terdiri dari komputer dan penyimpanan jaringan yang digunakan bisnis atau organisasi lain untuk mengatur, memproses, menyimpan, dan menyebarluaskan sejumlah besar data. Bisnis biasanya sangat bergantung pada aplikasi, layanan, dan data yang terdapat dalam pusat data, menjadikannya sebagai titik fokus dan aset penting untuk operasi sehari-hari.

Di jaringan memiliki banyak sumber daya yang perlu dikelola dengan baik. Ada file server, printer, intranet, scanner, dan berbagai perangkat lainnya yang digunakan oleh user di jaringan. Semua sumber daya tersebut bisa diatur oleh Active Directory, siapa saja yang boleh menggunakannya dan kapan sumber daya tersebut boleh digunakan. Tidak hanya itu, siapa saja yang mengelola sumber daya tersebut juga bisa diatur. Misalnya siapa saja yang boleh mereset password seorang user juga bisa diberikan hak untuk melakukan hal tersebut. Ini membuat Active Directory bisa diandalkan untuk membantu pekerjaan sebagai seorang Administrator. Selain itu hal yang berkenaan dengan optimalisasi lalu lintas jaringan juga bisa diatur oleh Active Directory.

Untuk melakukan pengamanan data, diperlukan adanya alat bantu yang dapat digunakan untuk mengatur keamanan dan beberapa kebijakan lainnya didalam program Microsoft windows. Group Policy menyediakan cara yang mudah dan efektif untuk mengelola preferensi dan pengaturan untuk komputer dan pengguna. Dengan Group Policy operator dapat mengelola preferensi dan pengaturan untuk ribuan pengguna atau komputer dengan cara yang sama seperti operator mengelola preferensi dan pengaturan untuk satu komputer atau pengguna dan tanpa pernah meninggalkan meja operator. Untuk melakukan ini, operator menggunakan salah satu dari beberapa alat manajemen untuk mengubah preferensi atau pengaturan ke nilai yang diinginkan, dan perubahan ini diterapkan di seluruh jaringan ke subset dari komputer dan pengguna yang ditargetkan.

Group Policy Management menyediakan cara yang sangat sederhana untuk melihat apa yang terjadi dalam satu Group Policy Object (GPO) tertentu. Namun, dalam satu GPO memiliki kemampuan untuk membuat banyak perubahan konfigurasi. Default Domain Policy, misalnya sudah dikonfigurasi dengan opsi tertentu, terutama ditujukan untuk keamanan. Berdasarkan pada permasalahan yang telah diuraikan diatas maka penulis mengajukan tugas akhir dengan judul "Membangun Sistem Keamanan Pusat Data Menggunakan *Group Policy Management*".

2. METODE PENELITIAN

Dalam suatu perancangan sebuah sistem diperlukan suatu analisa yang tujuannya untuk menentukan suatu kebutuhan dari sistem itu sendiri. Pada bab ini peneliti akan menjelaskan bagaimana analisa proses pembangunan sistem keamanan pusat data menggunakan Group Policy Management. Tujuan dari pembangunan sistem ini untuk memberikan keamanan pada pusat data dari tindakan user dalam memindahkan atau menduplikasikan data dari komputer client ke perangkat lain. Seperti contoh: copy data ke flashdisk, floppy disk, CD atau DVD.

Dalam penelitian pembangunan sistem keamanan tersebut menggunakan Group Policy Management yang dapat mengatur sistem pekerjaan yang dibuat oleh server

.

untuk client tersebut. Dalam sistem tersebut dapat diartikan bahwa apapun aktivitas yang dilakukan oleh client dapat dibatasi oleh server. Dengan demikian client tidak mudah untuk melakukan aktivitas yang dilakukan secara bebas mungkin seperti mengambil data dari komputer client. Perangkat lunak yang digunakan menggunkan sistem operasi Windows Server 2012 sebagai wadah pembangunan sistem keamanan agar dapat melakukan kofigurasi-konfigurasi sistem tersebut.

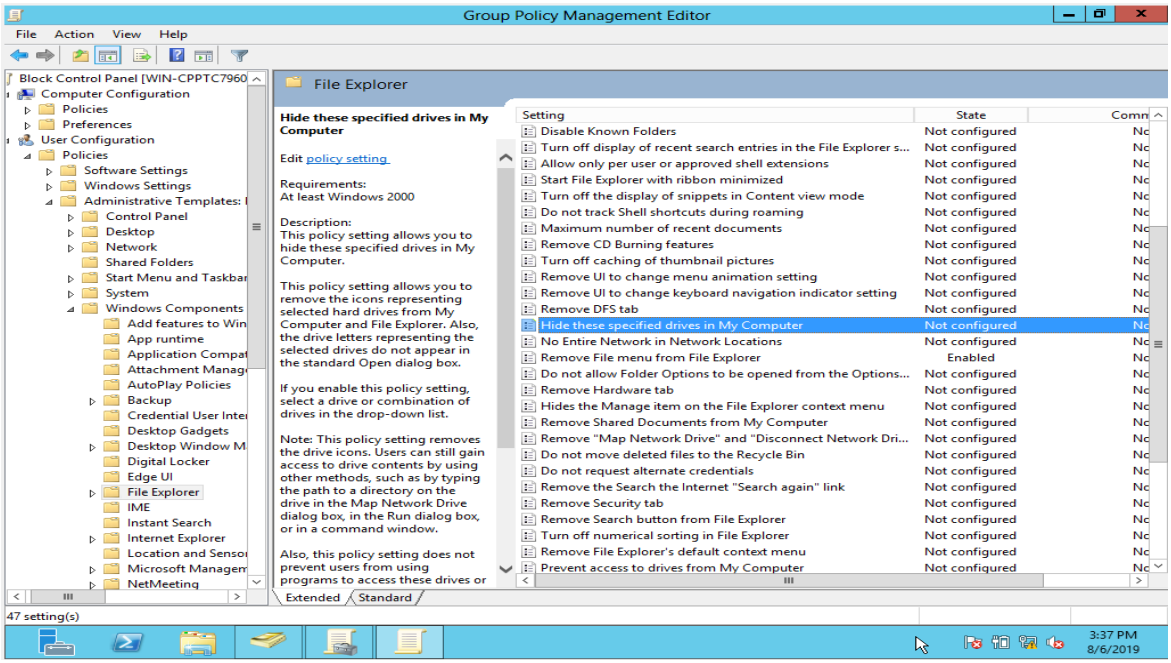
3. HASIL DAN PEMBAHASAN

Hasil pembahasan berdasarkan perancangan yang telah dibuat sebelumnya. Pada bagian ini sebelumnya akan dilakukan pengujian sistem keamanan Pusat Data apakah dapat berjalan sesuai dengan keinginan. Pengujian yang akan dilakukan merupakan pengujian beberapa komponen penting dalam sistem keamanan Pusat Data.

Berikut ini adalah pengujian hasil dari sistem dari layanan kebijakan GPM melalui server. Sistem yang dibuat antara lain bagaimana cara menerapkan layanan kebijakan GPM dari server terhadap *client*. Peneliti akan menguji dan menerapkan layanan-layanan kebijakan diantaranya, sebagai berikut:

1. Menyembunyikan *drive My Computer* pada komputer *client*.
2. Mencegah *client* mengakses *drive local computer* dan penyimpanan external lainnya.
3. Mencegah *client* untuk membuka *map drive* dengan izin *username* dan *password*.
4. Memblokir akses *Control Panel*.
5. Menyembunyikan dan *disable* seluruh *icon* yang ada pada *desktop client*.

Pada gambar 1 adalah tampilan layanan kebijakan dari GPM. Banyak yang dapat dilakukan untuk menerapkan layanan-layanan kebijakan yang terdapat didalamnya.



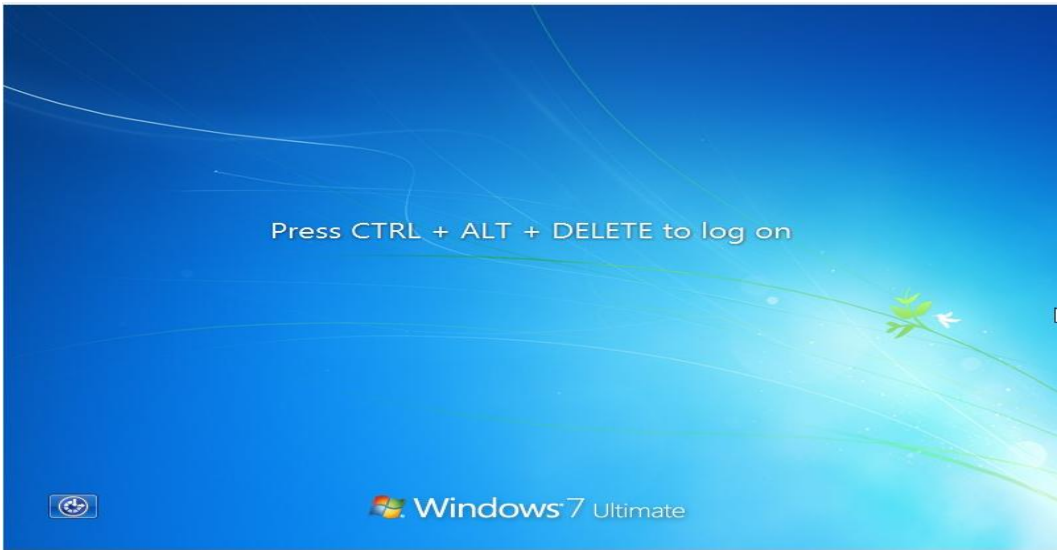
Gambar 1. Tampilan Layanan- Layanan Kebijakan GPM

JIKSTRA Vol. 6, No. 01, April 2024 *Halaman. 85-95*
p-ISSN :2715-887X
e-ISSN: 2747-2485

Selanjutnya adalah pengujian tampilan hasil dilakukan setelah menguji sistem dari aturan layanan GPM. Pengujian dilakukan untuk mengetahui apakah perancangan sistem keamanan yang telah dibuat dapat berjalan dengan baik dan sesuai dengan yang diinginkan. Langkah-langkah untuk *login* dan menguji hasil yang telah dibuat adalah, sebagai berikut:

1. Langkah-langkah *login* komputer *client*, diantaranya:

   a. Tampilan seperti yang terdapat pada gambar 2 adalah awal untuk masuk ke tampilan *desktop*. Untuk melanjutkannya yaitu dengan cara menekan tombol CTRL+ALT+*DELETE*, kemudian akan masuk ke tampilan berikutnya.



Gambar 2. Tampilan Awal *Log On* Komputer *Client*

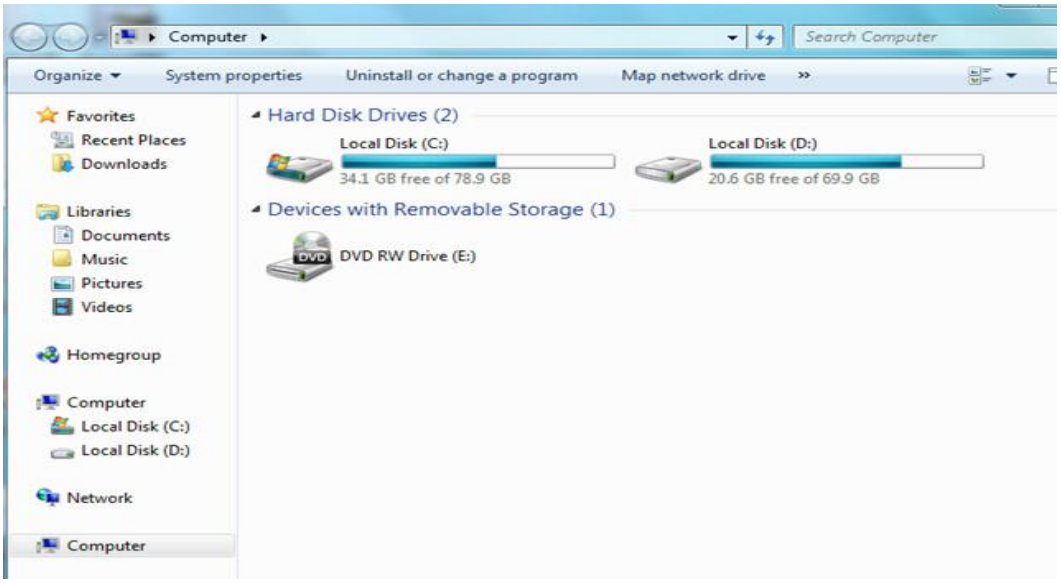
   b. Kemudian langkah selanjutnya akan masuk pada tampilan untuk memasukkan *username* dan *password* seperti gambar 3 Pada tampilan ini diwajibkan untuk memasukkan *username* dan *password* yang telah terdaftar pada *server*.

.

Gambar 3. Tampilan *Input Username* Dan *Password*

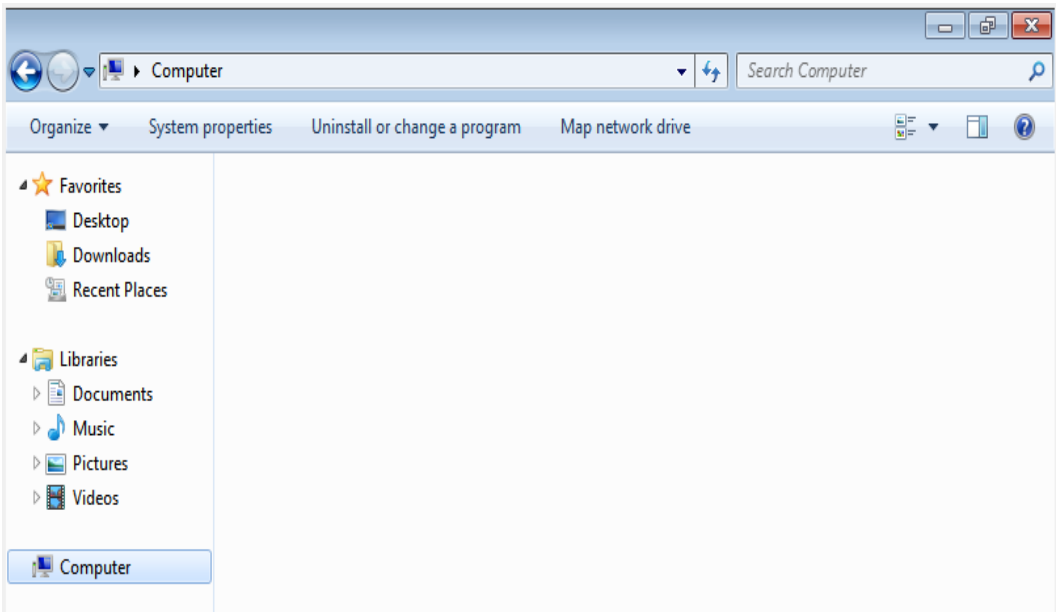
c. Setelah berhasil *log on* akan masuk pada tampilan *desktop* yang sudah diterapkan layanan-layanan kebijakan GPM dari *server*.

2. Hasil-hasil yang telah diterapkan layanan-layanan kebijakan GPM pada *client* adalah, sebagai berikut:
   a. Menyembunyikan *drive My Computer* pada komputer *client*.
   Pada gambar 4 adalah tampilan sebelum diaktifkan layanan kebijakan GPM. Terlihat bahwa masih ada *drive* pada *My Computer*.



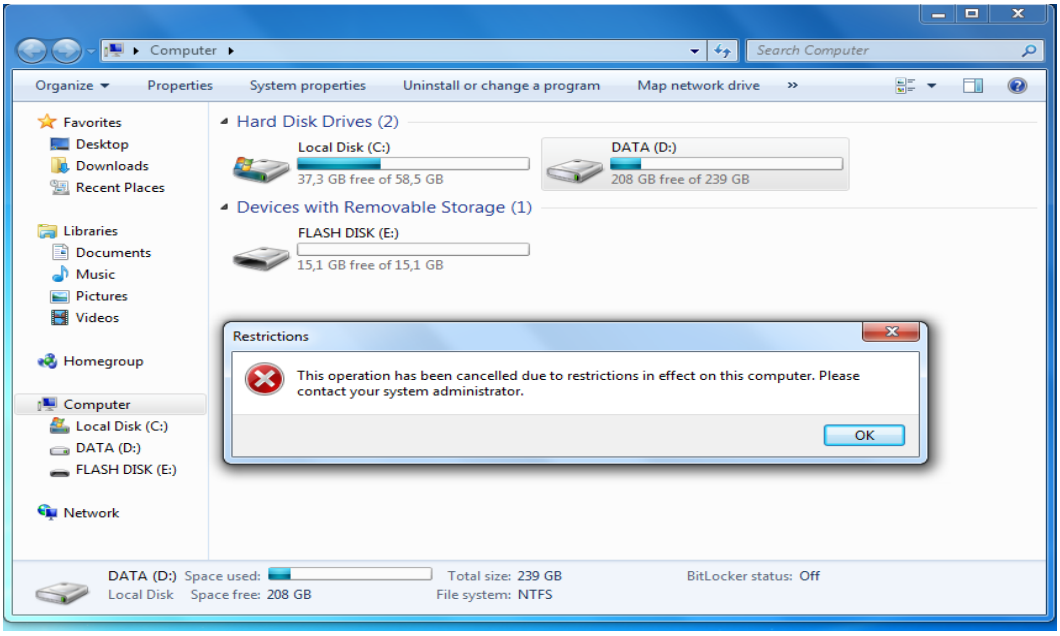
Gambar 4. Tampilan *Drive* Sebelum Disembunyikan

Pada gambar 5. adalah hasil dari layanan kebijakan GPM terlihat bahwa sama sekali tidak dapat dibuka dan tidak terlihat sekalipun (disembunyikan) *drive* pada *My Computer* dikomputer *client*.



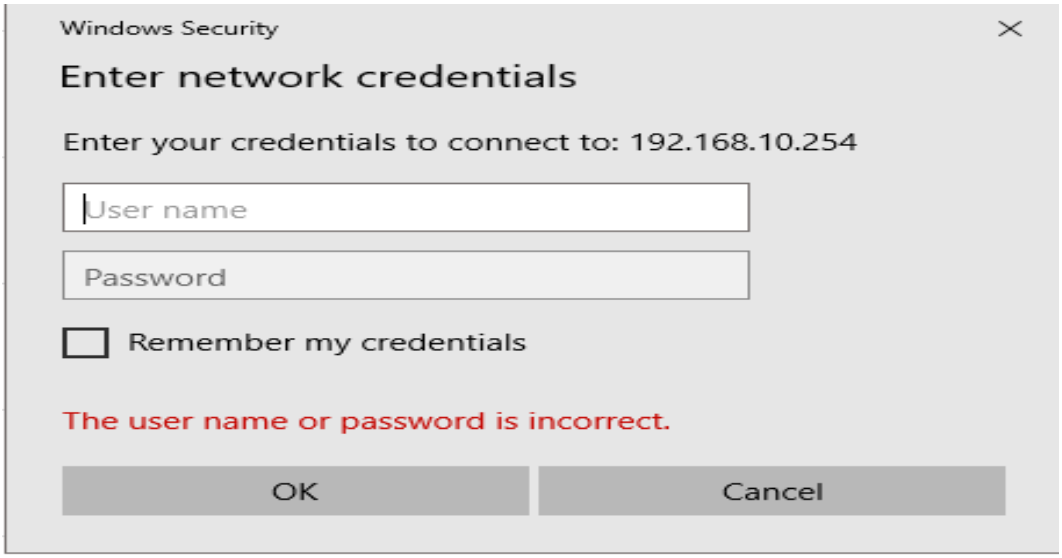
Gambar 5. Tampilan Sesudah Disembunyikan

b. Mencegah *client* mengakses *drive local computer* dan penyimpanan lainnya. Pada layanan ini *client* hanya dapat melihat *folder drive* saja, tetapi tidak dapat membukanya dan mengaksesnya sama sekali. Seperti yang terlihat pada gambar 6 berikut ini.



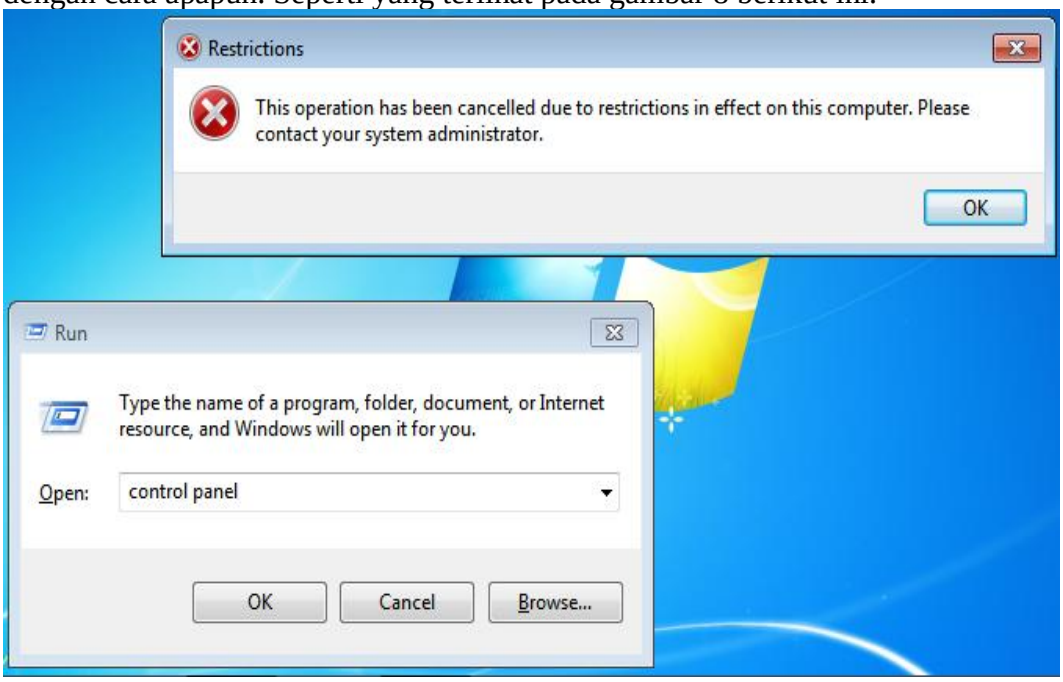
Gambar 6. Tampilan Mencegah Akses *Drive Local Computer*

c. Mencegah *client* untuk membuka *map drive* dengan izin *username* dan *password*. Jika *client* membuka *map drive* atau *folder* yang ada pada *server* dikomputer *client*, maka harus memasukkan *username* dan *password* yang terlihat pada gambar 7 berikut ini.



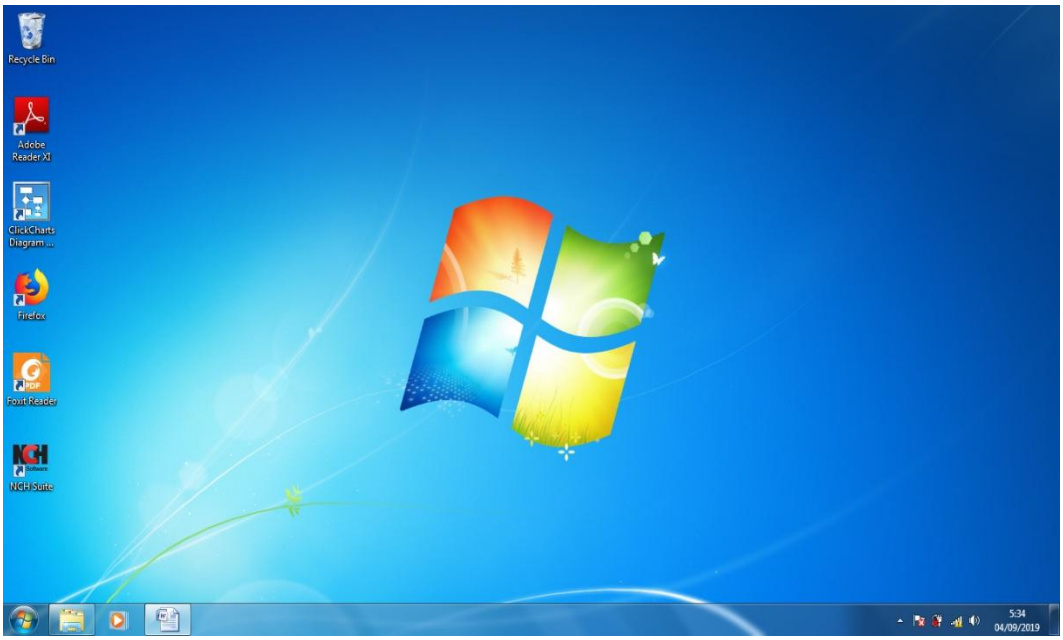
Gambar 7. Tampilan Izin Membuka *Map Drive*

d. Memblokir akses *Control Panel*.
Pada layanan ini *client* tidak dapat membuka dan mengakses menu *Control Panel* dengan cara apapun. Seperti yang terlihat pada gambar 8 berikut ini.



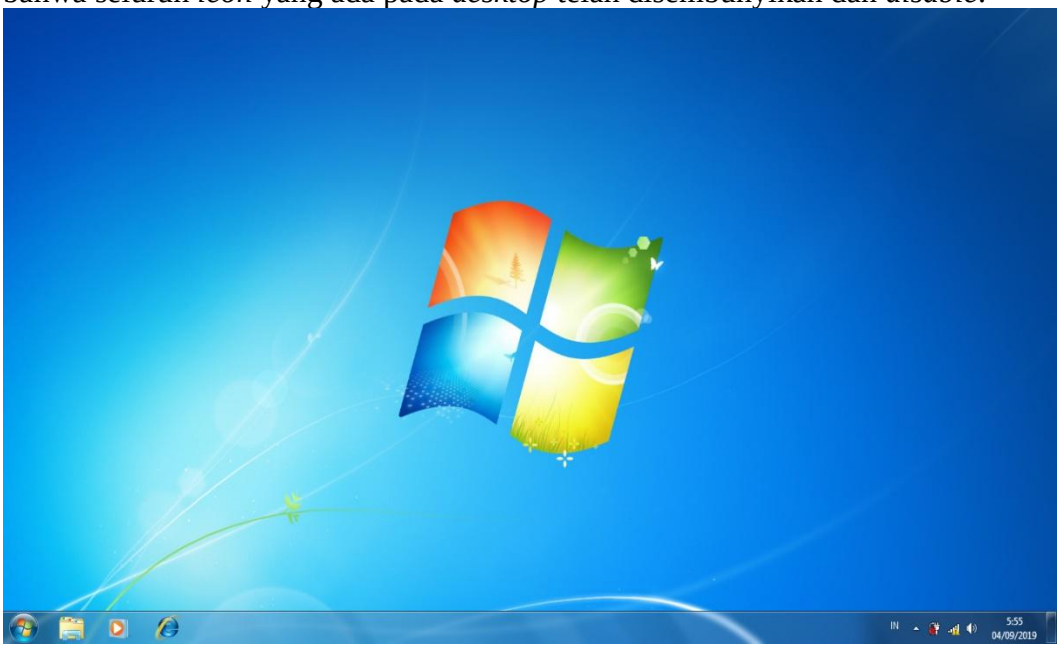
Gambar 8. Tampilan *Block Control Panel*

e. Menyembunyikan dan *disable* seluruh *icon* yang ada pada *desktop client*.
Pada gambar 9 adalah tampilan *icon* yang belum diaktifkan layanan kebijakan GPM. Terlihat bahwa masih terlihat *icon* yang ada pada *desktop*.



Gambar 9. Tampilan *Icon* Sebelum Disembunyikan

Pada gambar 10 adalah layanan kebijakan GPM yang sudah diaktifkan. Terlihat bahwa seluruh *icon* yang ada pada *desktop* telah disembunyikan dan *disable*.



Gambar 10. Tampilan Sesudah *Disembunyikan* dan *Disable*

Apabila *server* menerapkan layanan kebijakan *Group Policy Management* terbaru, maka *client* wajib melakukan *restart* dan *log on* ulang kembali agar ditempatkan pada aturan terbaru.

4. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan terhadap model rekonstruksi menggunakan inverse backpropagation dapat dilihat bahwa perbedaan atau selisih antara hasil rekonstruksi pada inverse backpropagation memberikan hasil yang lebih baik dibandingkan dengan rekonstruksi menggunakan Bilinear interpolation biasa dimana pada semua citra pengujian nilai MSE dan PSNR pada rekonstruksi inverse backpropagation memberikan nilai yang lebih baik dibandingkan dengan rekonstruksi menggunakan Bilinear interpolation biasa. Hal ini dapat dilihat dari perhitungan nilai MSE dan PSNR antara rekonstruksi menggunakan Bilinear interpolation dan model inverse backpropagation. Pada nilai MSE, model inverse backpropagation memberikan penurunan terendah sebesar 1.98 % dari pengujian 1 dan penurunan terbesar sebesar 40.25 % dari pengujian 3. Pada nilai PSNR, model inverse backpropagation mampu memberikan peningkatan terendah sebesar 0.44 % dari pengujian 1 dan peningkatan terbesar sebesar 9.72% dari pengujian 3 sehingga secara garis besar model inverse backpropagation yang digunakan pada penelitian ini dapat memberikan peningkatan kualitas pada rekonstruksi citra menggunakan bilinear interpolation.

DAFTAR PUSTAKA

[1] Alim, Z., Cancer, Y., Utara, U. S., & Teori, L. (2016). MENINGKATKAN KEAMANAN DATA CLOUD COMPUTING MENGGUNAKAN, V(1), 23–27.

[2] Bilal Syahid. (2019, Juni 30). Pengertian Data. Guru Pendidikan. Diakses dari https://www.gurupendidikan.co.id/data/

[3] Dewannanta, D. (2007). Perancangan Jaringan Komputer – Data Center, 1 – 6.

[4] Diansyah, T. M., Informatika, J. T., Tinggi, S., & Harapan, T. (2015). Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan wireshark, IV(2), 20–23.

[5] Havia, T., Managed, C., & Services, B. (2013). Microsoft Windows Server 2012, (May).

[6] Ilmu, F., Universitas, K., Unggul, E., & Jeruk, K. (2016). PEMANFAATAN FLOWCHART UNTUK KEBUTUHAN DESKRIPSI, 12, 21–26.

[7] Informatika, D. M., Teknik, F., & Surabaya, U. N. (n.d.). (2016). IMPLEMENTASI

APLIKASI MANAJEMEN PENGGUNA DAN GRUP BERBASIS ACTIVE DIRECTORY MENGGUNAKAN TEKNOLOGI .NET, No Title, 7–15.

[8] J. Petter, B. Ronald, B. Wayne, D. (2009). Windows Server 2008 (Pearson Education). 800 East 96th Street, Indianapolis, Indiana 46240 USA: SAMS

[9] Margar Rouse. (2012, Februari). Group Policy Management Console. TechTarget. Diakses dari https://searchwindowsserver.techtarget.com/definition/Group-Policy-Management-Console

[10] Pandey, S. (2011). MODERN NETWORK SECURITY : ISSUES AND CHALLENGES, 3(5), 4351–4357.

[11] Priatmoko, D. B. (n.d.). (2016). UNTUK MELINDUNGI DATA ORGANISASI (Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI) IKIP PGRI MADIUN), 40(1), 160–169.

[12] Rifzan (2018, Desember 26). Pengertian Database dan Fungsinya. Robicomp. Diakses dari https://www.robicomp.com/pengertian-database-dan-fungsinya.html

[13] Russel Smith, (2014, Desember 22). How to Use Starter Group Policy Objects in Windows Server. Petri IT Knowledgebase. Diakses dari https://www.petri.com/how-to-use-starter-group-policy-objects-in-windows-server

[14] Sari, M. (n.d.). (2017). IMPLEMENTASI PEMBATASAN AKSES PEMAKAI KOMPUTER MENGGUNAKAN GROUP POLICY OBJECT DI WINDOWS SERVER 2012 R2.