PEMANFAATAN KEYLOGGER BERBASIS SPYWARE UNTUK MEMONITORING AKTIVITAS PENGGUNAAN KEYBOARD USER

Asep Saefullah[1*]; Billy[2]; Fabrielo Hanielus Caezario Talumepa[3]
[1,2,3]Prodi Teknik Informatika, Universitas Matana
**E-mail : asaefullah@gamil.com*

Abstrak

Menambahnya pemilik komputer membuat pengguna kurang atau lebih memiliki pengaruh kepada sejumlah pengguna yang berinteraksi dengan komputer. Berdasarkan dari hasil penelitian yang dilakukan oleh National Center Education Statistics (NCES, 2003). Penggunaan internet oleh pengguna dibedakan dengan bagaimana pengguna menggunakannya, apakah dari pengguna menggunakannya untuk fasilitas chatting, email, tugas, browsing untuk mendapatkan informasi, termasuk bermain game online. Tetapi tidak semua konten yang ada berisikan informasi yang edukatif, dan juga terdapat banyak sekali informasi negative yang tidak sesuai yang dapat diakses oleh anak-anak. Pengawasan terhadap penggunaan teknologi informasi sangatlah dibutuhkan karena perkembangan ilmu pengetahuan mengenai pembuatan virus, worm, atau spyware. Menginstalasi antivirus adalah solusi untuk mencegahnya virus mengkontaminasi jaringan ataupun sistem komputer. Namun dengan demikian antivirus-pun tidak dapat memantau aktifitas pengguna, dengan kata lain, kegiatan penggunaan keyboard. Keylogger dapat mampu merekan semua aktivitas keyboard. Keylogger harus diinstal pada komputer yang ditargetkan untuk merekam aktivitas penggunaan keyboard. Kemudian untuk dapat mengambil file log, Keylogger harus memiliki akses secara fisik ke dalam komputer. Dengan ini sebagai dasar untuk membuat sebuah ide untuk memantau aktivitas keyboard pengguna. Tetapi jika hanya ini, pasti akan menimbulkan masalah jika pengguna mengetahui tentang adanya keylogger. Untuk mengatasi masalah ini, menciptakan sebuah program yang dapat memantau aktivitas pengguna saat mengakses komputer atau dalam hal ini apa yang pengguna ketikkan untuk memberikan hak-hak istimewa untuk mengetahui apa yang pengguna telah lakukan selama penggunaan. Mengingat cara ini, memberikan admin memantau pengguna saat mengakses komputer.

Kata kunci : *keylogger, komputer, monitor, keyboard, pengguna*

1. PENDAHULUAN

The National Center for Education Statistic (NCES) adalah badan federal utama untuk mengumpulkan, menganalisa dan melaporkan data yang terkait dengan pendidikan di Amerika dan negar-negara lainnya. Untuk memenuhi tugas dari kongres dalam mengumpulkan, menyusun, menganalisa dan melaporkan penuh dan lengkap kondisi yang berada di Amerika. Melakukan dan mempublikasikan analisis laporan khusus serta membantu negara dan lembaga setempat dalam meningkatkan sistem statistik serta ulasan dan melaporkan kegiatan pendidikan di luar negeri.

Menurut hasil survei dari *National Center Education Statistic* (NCES,2003), rumah dan sekolah adalah tempat utama anak-anak dan remaja menggunakan komputer, 81 persen dari anak usia (5 - 17) tahun menggunakan komputer disekolah dan 65 persen menggunakan komputer dirumah secara umum penggunan komputer disekolah lebih banyak dari pada dirumah. Segmentasi penggunaan internet pada remaja di rentang usia ini sebanyak 42 persen menggunakannya untuk menyelesiakan tugas sekolah, sementara 38 persen menggunakan sarana email atau *chatting* termasuk didalamnya adalah bermain *game online*, dan 22 persen selanjutnya menggunakan internet untuk *browsing* dan mencari informasi.

Mengingat dari waktu ke waktu, kepemilikan komputer semakin meningkat tiap tahun, sedikit banyak akan mempengaruhi jumlah pengguna yang berinteraksi dengan internet. Bermacam-macam konten di internet misalnya, tidak semua konten berisi hal-hal berbau pendidikan maupun pengetahuan yang bisa digunakan sebagai wawasan belajar, namun banyak juga konten - konten yang berisi infomasi negatif yang tidak selayaknya diakses oleh seorang anak dan remaja. Oleh karena itu, akibat dari meningkatnya peran komputer rumah dan

informasi yang beragam dalam kehidupan anak-anak maupun remaja maka diperlukan sebuah perhatian khusus.

Dari permasalahan diatas maka diperlukan suatu cara yang mampu memantau aktifitas pengguna pada saat mengakses komputer. Dengan adanya cara ini, maka memantau aktifitas pengguna dalam penggunaan komputer dan akses internet tidak akan terlewatkan.

2. METODOLOGI

2.1 SPYWARE

Serangan virus, *spyware* dan program membahayakan lainnya semakin meningkat kuantitas maupun kualitasnya. Hal tersebut terjadi karena semakin berkembangnya ilmu tentang *security komputer* dan kelemahan –kelemahan yang ditemukan dalam sebuah sistem.

Spyware adalah program yang mampu memata-matai aktivitas pengguna komputer, di mana salah satunya adalah dapat merekam ketikan *keyboard* yang disebut *keylogger*.

(Kurniawati, 2010) *keylogger* adalah program untuk memonitor(memantau) segala aktifitas yang dilakukan oleh pengguna komputer, jenis *keylogger* yang ada adalah *keylogger hardware* berupa sebuah bentuk fisik dari *keylogger* yang hanya dapat merekam aktifitas yang terjadi jika pengguna mengetik menggunakan *keyboard* fisik tetapi tidak dengan menggunakan *keyboard* maya. *Keylogger software* berupa aplikasi yang nantinya akan diinstal pada komputer yang mampu merekam segala inputan dari *keyboard*. Untuk dapat merekam segala aktifitas *keyboard, keylogger* harus dijalankan setelah sistem operasi berjalan dan masuk pada tampilan desktop. Karena *keylogger* merupakan perangkat lunak yang bersifat memantau maka *keylogger* akan dijalankan secara *background process* dan tidak diketahui oleh pengguna yang menggunakan komputer tersebut.

Ada lima metode yang banyak digunakan oleh perangkat lunak *keylogger* diantaranya *hypervisor-based*, *kernel-based*, *hook-based*, *passive method*, dan *form grabber based*. Kemudian diantara lima metode tersebut *passive method* adalah teknik yang paling banyak digunakan oleh pembuat *keylogger*. Metode ini banyak menggunakan fungsi Windows API(*Appication Programming Interface*).

Jika *keylogger* tersebut dapat dimanfaatkan untuk aktivitas positif yaitu monitoring jaringan area lokal (LAN), maka hal itu akan memudahkan seorang *Administrator* dalam mengawasi jaringan komputer yang dikelolanya. Aktivitas yang diawasi misalnya untuk mengawasi bawahannya saat bekerja hingga memang berniat untuk mencuri data pribadi seseorang.

Ada dua istilah lain yang berkaitan dengan *spyware* yaitu *trojan horse* dan *Remote Administration Tool* (RAT). *Trojan horse* adalah program yang disamarkan dengan file lain yang tidak dianggap berbahaya contohnya *icon* program yang sama dengan icon MS.Word ditambah dengan nama file yang sangat menarik sehingga memancing user untuk mengeksekusi file tersebut.

Biasanya tiap *spyware* yang disebarkan diberikan kode yang unik untuk membedakan informasi dari tiap target dengan menggunakan metode *Globally Unique IDentifier* (GUID). GUID akan menyimpan informasi *cookie* dan perangkat keras pada *harddisk* komputer target. *Spyware* secara periodik akan terus – menerus mengirimkan informasi tersebut sehingga informasi yang dimiliki oleh pemilik *spyware* akan diperbarui terus. (Ari, 2006)

Pemanfaatan *SPYWARE* Berbasis *Client-Server* untuk Monitoring Aktifitas Keyboard

Dengan apa yang peneliti ketahui maka dari masalah yang ada peneliti ingin membuat program yang dapat melakukan suatu *log* untuk dapat memantau apa yang dilakukan oleh setiap pengguna atau *user* yang menggunakan komputer maupun laptop yang sudah dipasangi sebuah program login seperti dalam warung internet atau yang disering disebut sebagai warnet. Dengan terpasangnya program maka *admin* dapat melihat aktifitas apa saja yang dilakukan *user* dan dapat menanggulangi jika ada aktifitas yang mencurigakan yang dilakukan pengguna tersebut selama menggunakan komputer dan dapat membantu melihat jika perangkat mengalami kerusakan jika sehabis dipakai pengguna mengalami kerusakan.

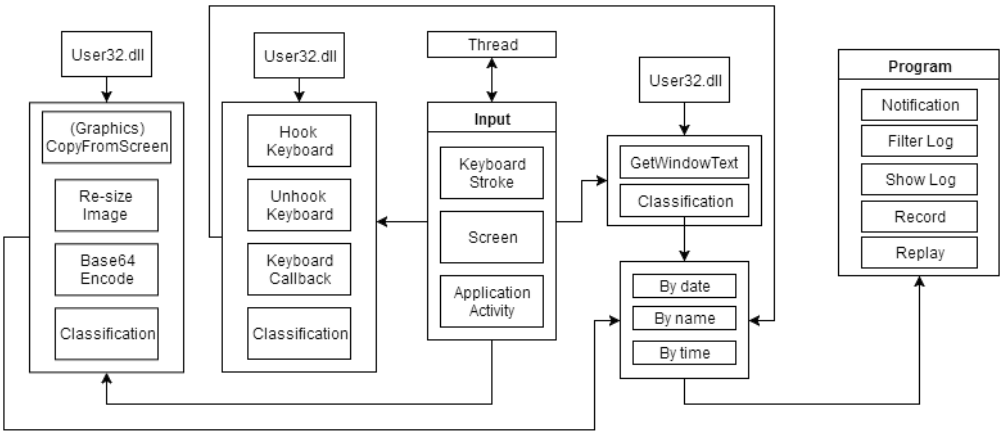
Gambar 1. Ilustrasi Spyware

2.2 Literature Review

1. Penelitian yang dilakukan oleh Mulki Indana Zulfa dari Teknik Elektro Fakultas Teknik Universitas 17 Agustus 1945 Cirebon, Indonesia (2015) yang berjudul "Pemanfaatan Spyware Berbasis Client-Server untuk Monitoring Aktivitas Keyboard". Penelitian ini menggunakan Keylogger untuk mengetahui apakah *spy agent* dapat berhasil atau tidak dalam melakukan *logging keyboard* dari *client-server*.
2. Penelitian yang dilakukan Ruchi Jain dan Dr. Mohd Amjad dari Department of Computer Science Engineering/Information Technology Al Falah School of Engineering and Technology, Jamia Millia Islamia New Dehli (2014) yang berjudul "Computer Surveillance System". Penelitian ini berisikan tentang cara pemantauan komputer dan pemanfaatan Computer Surveillance System untuk pengguna (user).
3. Penelitian yang dilakukan oleh Azwar Anas, Anjik Sumaaji, S.Kom.,M.Eng, dan Teguh Sutanto,M.Kom.,MCP (2012) dari Sistem Informasi STIKOM Surabaya, Indonesia yang berjudul "Rancang Bangun Aplikasi Pengintai Aktifitas Komputer Menggunakan Layanan Cloud To Device Messaging (C2DM) Pada Smartphone Android". Penelitian ini berikan mengenai pemanfaatan *Keylogger* pada pengguna hanphone untuk mengetahui apa saja yang pengguna (anak-anak) lakukan.
4. Penelitian yang dilakukan oleh Preeti Tuli dan Priyanka Sahu dari Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India (2013) yang berjudul "System Monitoring and Security Using Keylogger". Penelitian ini menggunakan program Keylogging yang bertujuan untuk mengetahui manfaat yang didapatkan dari monitoring jaringan sistem dari suatu perusahaan yang digunakan oleh karyawan.
5. Penelitian yang dilakukan oleh Tri Wahyu W, Aidil Sanjaya dari Teknik Informatika, Fakultas Teknologi Komunikasi Informatika, Universitas Nasional, Indonesia (2008). Penelitian ini mengenai pentingnya keamanan dalam menghadapi software-software yang dapat meng-invasi *PC* pengguna.

Dari kelima literature membantu dalam pembahasan yang peneliti ingin bahas dan ingin berikan penjelasan. Salah satu dari literature di atas terdapat suatu studi yang mirip dengan penilitian yang dilakukan oleh peniliti. Judul penelitian tersebut adalah "Rancang Bangun Aplikasi Pengintai Aktifitas Komputer Menggunakan Layanan Cloud To Device Messaging (C2DM) Pada Smartphone Android", dengan penelitian peneliti yaitu "PEMANFAATAN KEYLOGGER BERBASIS SPYWARE UNTUK MEMONITORING AKTIVITAS PENGGUNAAN KEYBOARD USER". Perbandingan tersebut meliputi kegunaan dalam pemanfaatan, target dari program yang telah dibuat dan juga teknologi yang dipakai.

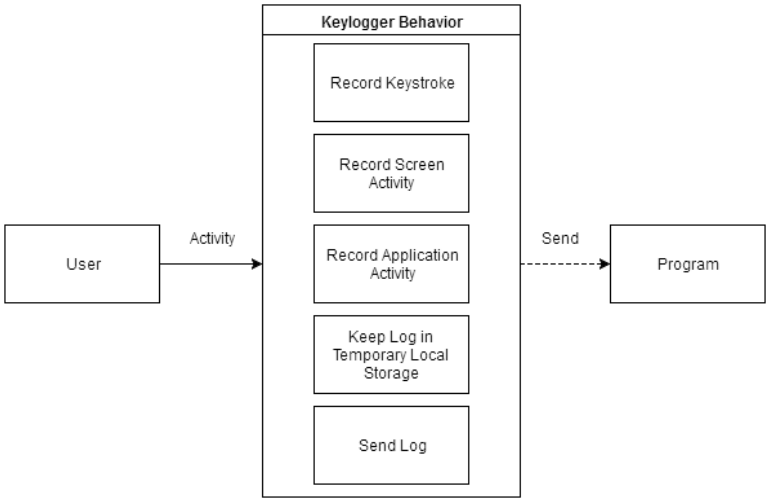
2.3 **Gambaran Umum Program**



Gambar 2. Gambaran Umum Program ke Program

Konsep dalam pembuatan program ini adalah membuat aplikasi yang dapat berjalan tanpa di ketahui oleh pengguna, sesuai dengan namanya untuk memantau aktifitas pengguna. Aplikasi ini jika terlacak atau diketahui oleh pengguna maka yang akan dilihat pengguna adalah sebagai salah satu program atau *service* yang berjalan di belakang layar dengan melakukan fungsi sebagai memonitor jaringan komputer dikarenakan sifat keylogger yang mirip dengan *logging* setiap ketikan yang dilakukan pengguna dari pengguna hanya akan melihat statistika yang dijalankan pengguna.

2.4 Use Case Diagram



Gambar .3. Use Case Diagram Keylogger

Tabel 1 Penjelasan singkat *Use Case Diagram Keylogger* aplikasi desktop *keylogger*

Nama Use Case	Deskripsi
Record Keystroke	Proses yang meng-*capture* aktifitas penggunaan keyboard
Record Screen Activity	Proses yang meng-capture setiap aplikasi

	yang berjalan
Record Application Activity	Proses yang merekam segala aktifitas aplikasi
Keep Log in Temporary Local Storage	Proses yang digunakan untuk menyimpan sementara *log* yang dihasilkan pada penyimpanan lokal sebelum dikirim ke program
Send Log	Proses yang menangani pengiriman *log* ke *server via* internet/dapat menggunakan jaringan lokal sebagai jaringan offline tanpa menggunkan internet

Gambaran *Use Case Diagram Keylogger* pada gambar 3, memberikan *Record Keystroke* sebuah proses untuk meng-*capture* aktifitas penggunaan *keyboard user*. Penggunaan di sini dapat berlaku dalam penggunaan *keyboard* dalam apapun jenisnya karena penggunaan *keylogger* di sini merupakan *keylogger* yang dapat melakukan *log* berbagai aktifitas *software* maupun *hardware* kecuali jika menggunakan *keylogger hardware* yang dimana dapat melakukan *log* untuk secara *hardware* saja.

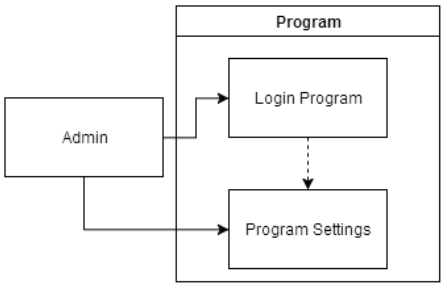
Gambar 4 Ilustrasi *Keylogger Hardware [14]*

Record Screen Activity Keyboard merupakan sebuah proses yang meng-capture setiap aplikasi yang berjalan pada komputer yang digunakan atau diaktifkan oleh *user* tetapi bukan yang berjalan pada *background-activity* karena *background activity* tidak terekam oleh *keylogger* karena dinilai sebagai *system* yang berjalan di luar dari pengguna atau *user*. Record Application Activity merekam segala aktifitas aplikasi yang memiliki sifat aktif dari pada program yang dijalankan oleh pengguna dan bukan dari pada *background activity* seperti yang sudah dijelaskan pada sebelumnya. Keep Log in Temporary Local Storage sebuah proses yang digunakan untuk menyimpan sementara *log* yang dihasilkan oleh *keylogger* pada penyimpanan local komputer/sistem sebelum dikirimkan ke program untuk diolah dan disajikan kepada *admin* untuk sebagai data yang ditangkap/direkam oleh *keylogger*. Send Log adalah sebuah proses yang menangani pengiriman *log* ke *server*(dalam hal ini adalah *server* yang dimaksud merupakan *server admin*) via internet(jaringan tanpa kabel atau nirkabel) /dapat menggunakan jaringan lokal (*LAN/Local Area Network* dalam suatu tempat) sebagai jaringan *offline* tanpa menggunakan internet.

Tabel 2. Penjelasan singkat *Use Case diagram* Program untuk *Admin*

Nama Use Case	Deskripsi
Login Program	Proses yang menangani *login* pada program *keylogger* sebelum dapat melakukan pengaturan aplikasi *keylogger*

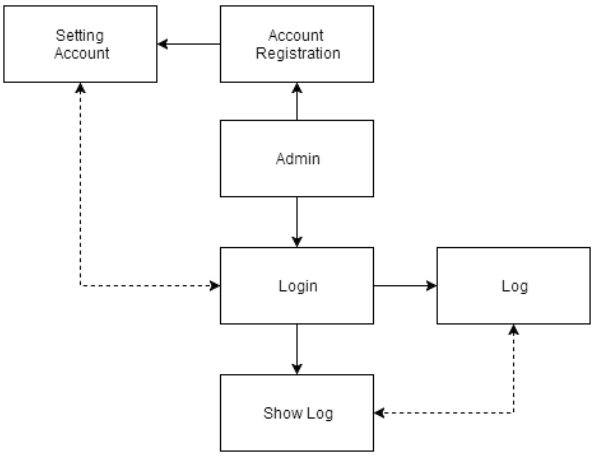
Program Settings	Proses yang menangani pengaturan aplikasi *keylogger*



Gambar 4. Gambaran Use Case Diagram Program

Login Program adalah proses yang menangani *login*(masuk ke dalam program dengan *privilege* atau dengan *setting* atau pengaturan yang berbeda-beda dari setiap *login admin* yang ada) pada program *keylogger* sebelum dapat melakukan pengaturan aplikasi *keylogger*.

Program Settings proses yang menangani pengaturan aplikasi *keylogger* sesuai yang diinginkan oleh *admin*.



Gambar 5 Gambaran Use Case Diagram Program

Tabel 3. Penjelasan Singkat *Use Case Diagram* Program

Nama Use Case	Deskripsi
Setting Account	Proses yang menangani pengaturan akun pemakaian
Account Registration	Proses yang menangani pendaftaran akun baru untuk menggunakan program
Login	Proses masuk atau menggunakan ke dalam program
Show Log	Proses yang menampilkan *log*
Log	Proses dimana user dapat memilih untuk menampilkan *log* sesuai waktu dan tanggal yang diinginkan

Setting Account adalah proses yang menangani pengaturan akun pemakaian yang dimiliki oleh seorang *admin* dapat juga melakukan pengaturan sesuai privilege yang ada.

Account Registration sebuah proses yang menangani pendaftaran akun baru yang ingin dibuat untuk menggunakan program dengan privilege yang diberikan kepada akun baru dari *admin* yang tertinggi atau pengguna yang memiliki akses program utama (*admin* utama).

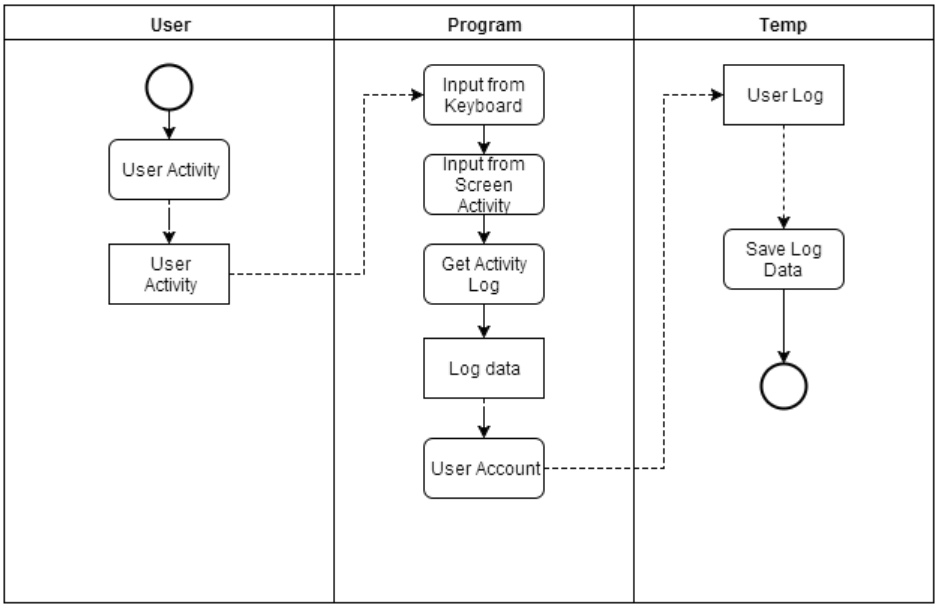
Login adalah proses masuk atau menggunakan ke dalam program yang bertujuan membedakan antara *admin* atau pengguna biasa.

Show Log adalah sebuah proses yang menampilkan *log*dari pada pengguna biasa yang telah terekam oleh program *keylogger* yang diinginkan oleh *admin* untuk dilihat, dapat melihat waktu dan juga urutan yang dilakukan oleh *user* sesuai dengan *log* yang sudah terekam sebelumnya.

Log adalah proses dimana user(dalam hal ini *user* adalah *admin* bukan pengguna biasa atau *user* biasa) dapat memilih untuk menampilkan *log* sesuai waktu dan tanggal yang diinginkan dari *log* yang ada, jika tidak ada maka *log* yang ditampilkan akan berupa kosong atau *Not-Available* atau *N/A*.

2.5 Activity Diagram

Pada *keylogger* proses perekaman pada aktifitas *keyboard* dimulai saat terdapat suatu interaksi dari pengguna yang memakai keyboard komputer atau disebut dengan *user activity*, *user activity* bisa berupa aktivitias yang terjadi saat keyboard komputer ditekan oleh pengguna dan berupa *screen capture* dari layar aplikasi yang sedang berjalan atau aktif dan hasilnya akan berupa data *log* dari semua aktifitas-aktifitas pengguna terkecuali aktifitas bukan dari pengguna, proses ini dilakukan secara otomatis oleh aplikasi. Selanjutnya aplikasi yang berjalan akan menambahkan informasi pengguna yang menggunakan komputer tersebut, data ini diambil dari *user account* masing-masing tiap komputer. Selanjutnya data-data *log* yang ada akan disimpan sementara pada lokal database sebelum dikirim ke aplikasi atau program utama.

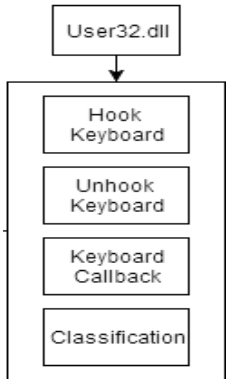


Gambar 6. Gambaran Activity Diagram Keylogger

Proses menampilkan *log* dimulai dari dari program yang telah menerima *log* dari aplikasi *keylogger* akan memberitahukan pada program bahwa ada *log* baru yang harus dimasukkan kedalam program, dari log yang didapat maka penerimaan dari log baru tersebut tidak akan memberikan suatu perubahan ataupun suatu aktivtas yang dapat diketahui oleh pengguna yang pada akhirnya akan diterima oleh admin. Log baru yang terdapat dalam program akan dilakukan pemrosesan agar pada saat admin melihat *log* yang masuk tidak akan kebingungan dalam menginpretasikan datanya. *Log data* tersebut bukan dalam bentuk yang mudah dilihat walaupun sudah diproses oleh program karena sifat dari keylogger yang merekam segala aktifitas *keyboard* yang dilakukan oleh pengguna. *Admin* yang ingin melihat lebih detail lagi informasi *log* dapat

memilih menu *preview log* pada program, selanjutnya permintaan akan diproses untuk dilakukan permintaan.

3. HASIL DAN PEMBAHASAN



Gambar 7. Diagram Keylogger (user)

Proses ini terjadi dilakukan ketika pengguna menekan setiap tombol di *keyboard*, kejadian ini ditangkap menggunakan fungsi *Hook Keyboard()* yang merupakan *Windows API* dari sistem operasi *windows*, oleh karena itu proses ini memerlukan *libraryuser32.dll* yang sudah disediakan *windows*.

```
'create the hook
  Public Sub HookKeyboard()
        Callback = New
KeyboardHookDelegate(AddressOf
KeyboardCallback)
  KeyboardHandle = SetWindowsHookEx(13,
callback,
Process.GetCurrentProcess.MainModule.BaseAddres
s, 0)
  End Sub
```

Selanjutnya fungsi *HookKeyboard()* akan memanggil setiap alamat pada tombol *keyboard* yang sebelumnya berbentuk karakter ASCII Hex untuk diubah menjadiASCII karakter, karena ASCII Hex berupa angka dan sulit untuk dibaca.Variabel pengganti karakter ASCII Hex ke bentuk ASCII karakter lebih lengkapnya dapat dilihat pada lampiran. Selanjutnya hasil dari fungsi *HookKeyboard()* akan diklasifikasikan berdasarkan nama *user account*, tanggal, waktu, judul aplikasi yaitu judul yang terdapat pada setiap aplikasi yang berjalan dan *log* dari inputan *keyboard* yang sudah berbentuk karakter string. Proses merekam aktifitas *keyboard* dapat dihentikan dengan cara memanggil fungsi *Unhook keyboard().*

```
Public Sub UnhookKeyboard()
        If (Hooked()) Then
            If
  UnhookWindowsHookEx(KeyboardHandle)
        <> 0 Then
                KeyboardHandle = 0
```

```
End If
End If
End Sub
```

4. KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan bahwa :

a. Dengan adanya penggunaan *keylogger* maka proses pengawasan aktifitas penggunaan komputer dapat dilakukan secara rutin dengan seminimal mungkin dalam pengecekan komputer tanpa melakukan pengecekan satu per satu komputer. Peran admin untuk memantau aktifitas penggunaan komputer oleh pengguna tidak susah.

b. Penggunaan *keylogger* dengan sebagai program spyware yang tidak memerlukan banyak resource.

DAFTAR PUSTAKA

Anas Azwar, Anjik Sukmaaji, S.Kom.,M.Eng, Teguh Sutanto, M.Kom.,MC (2012). "Rancang Bangun Aplikasi Pengintai Aktifitas Komputer Menggunakan LayananCloud To Deice Messaging (C2DM) Pada Smartphone Android". STIKOM Surabaya, Surabaya, Indonesia.

Wardana, Ari(2006). "PemrogramanVirus dan Spyware". Jasakom,Jakarta.

Fowler, Martin (2004).UMLDistilled Edisi 3 Panduan SingkatBahasa Pemodelan Objek Standar.ANDI: Yogyakarta, Indonesia.

Huang, Wei (2010). *Android CloudTo Device Messaging.* Mengambil sumber dari :http://androiddevelopers.blogspot.com/2010/05/android-cloud-to-device-messaging.htmldiakses 04-05-2011 pukul 11.00 WIB

Kurniawati, Dewi (2010).KegunaanKeylogger, Jurnal Teknologi Informasi. Indonesia.

Mulki Indana Zulfa (2015). "PEMANFAATAN SPYWARE BERBASIS CLIENT-SERVER UNTUK MONITORINGAKTIVITAS KEYBOARD". Cirebon, Jawa Barat.

Preeti Tuli dan Priyanka Sahu (2013). System Monitoring and Security Using Keylogger.Department Of Computer Science Dimat, CSVTU, Raipur, Chhattisgarh, India.

Ruchi Jain dan Dr. Mohd Amjad (2014). Computer Surveillance System. Al Falah School ofEngineering and Technology.

Ramadah, Kartika (2012).Pengenalan Webservers, Universitas Gunadarma, Indonesia.

[Wibowo, Arip (2011)Web Server. Diambil dari : http://unyildadakan.com/internet/webserver/diakses tanggal 06-05-2011pukul 19:00 WIB.

Ramadah, Kartika (2010).WebService diambil dari : http://kartikanurramadha.info/a/webservice.pdf diakses tanggal 19-07-2011pukul 22.00WIB.

Thomas W. Olzak (April 2008)."Keystroke Logging", Ohio, America.

Wardana, Ari (2006). "PemrogramanVirus dan Spyware". Jasakom, Jakarta.

Wahyu Tri W, dan Aidil Sanjaya (Juli 2008). "STUDI SISTEM KEAMANAN KOMPUTER". Universitas Nasional, Jakarta, Indonesia.