Keamanan pada Grid Computing ~ *Survey Paper*

Ghufran Ibnu Yasa
Fakultas Sains dan Teknologi UIN Ar-Raniry

Abstract: Grid computing provides high computing power, enormous data storage, and collaboration possibilities to its users. Grid computing is currently in the midst of evolving standards, inheriting and customizing from those developed in the high performance, distributed, and recently from the Web services community. Grid computing is widely regarded as a technology of immense potential in both industry and academia. Which this interest, security become necessery to provide authentication, authorization, resource protection, secure communication, data integrity, trust management and network security. This paper tells about progression of the security system on grid computing by conducting a survey of existing paper and applications have been developed.

Keywords: Grid Computing; Computer Security; Grid Security.

1. Pendahuluan

Grid computing merupakan penggunaan sumber daya yang melibatkan banyak komputer terpisah secara geografis namun tersambung pada saluran komunikasi untuk memecahkan persoalan komputasi skala besar. Pada pengembangannya *grid computing* difokuskan untuk meningkatkan kemampuan komputasi, akses data dan peningkatan kapasitas penyimpanan data[1].

Penggunaan *grid computing* saat ini tidak saja oleh para ilmuan yang memerlukan proses komputasi dan mengolah data yang besar, *grid computing* juga sudah digunakan oleh para pengembang untuk keperluan bisnis sehingga secara teknologi dan cara penggunaan sudah berkembang secara lebih baik. Menurut tulisan singkat dari Ian Foster, ada beberapa hal yang bisa dijadikan acuan untuk melihat apakah sebuah sistem itu adalah *grid computing* atau bukan, yaitu[1]:

1. Sistem tersebut melakukan koordinasi terhadap sumberdaya komputasi yang tidak berada dibawah suatu kendali terpusat.

Seandainya sumber daya yang digunakan berada dalam satu cakupan domain administratif, maka komputasi tersebut belum dapat dikatakan *grid computing*.

2. Sistem tersebut menggunakan standar dan protokol yang bersifat terbuka (tidak terpaut pada suatu implementasi atau produk tertentu). *Grid computing* disusun dari kesepakatan-kesepakatan terhadap masalah yang fundamental, dibutuhkan untuk mewujudkan komputasi bersama dalam skala besar. Kesepakatan dan standar yang dibutuhkan adalah dalam bidang autentikasi, otorisasi, pencarian sumberdaya, dan akses terhadap sumber daya.
3. Sistem tersebut berusaha untuk mencapai kualitas layanan yang canggih, (*nontrivial quality of service*) yang jauh diatas kualitas layanan komponen individu dari *grid computing* tersebut.

Ketika penggunaan *grid computing* semakin meluas, kebutuhan akan sebuah sistem keamanan yang baik dalam *grid computing* adalah sangat diperlukan. Memang semenjak awal, sistem keamanan adalah isu yang masih terus diperbincangkan oleh para pengembang, karena banyak permasalahan yang timbul akibat penggunaan sumber daya yang banyak dalam sebuah sistem *grid computing*. Beberapa hal yang menjadi perhatian dari segi keamanan pada sistem *grid computing* adalah:

1. Perlindungan terhadap data dan aplikasi ketika dieksekusi
2. Perlu autentifikasi yang handal untuk pengguna dan code.
3. Menjaga eksekusi node lokal yang diperintahkan oleh *remote system*
4. Adanya banyak admin dan user dan menggunakan kebijakan yang berbeda.

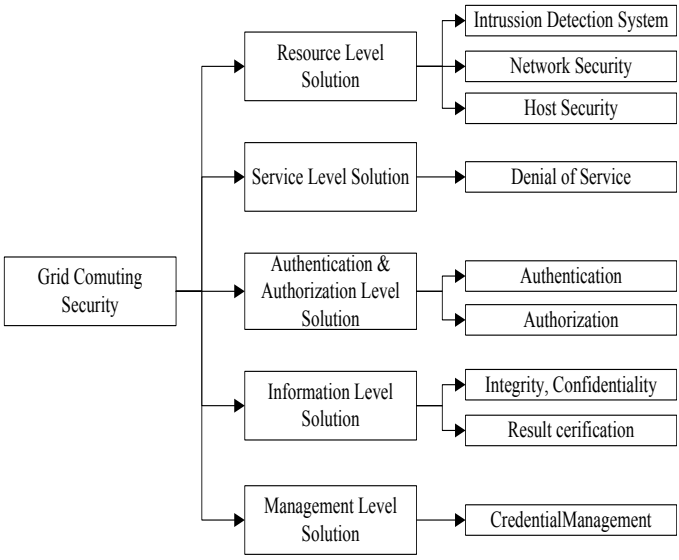
Ada beberapa model pendekatan yang digunakan dalam pengembangan kemanan pada *grid computing*. Salah satu yang saat ini menjadi acuan adalah usulan dari A. Bendahmane dkk, dalam tulisannya mengusulkan pembagian mekanisme dan solusi kemanan pada komponen yang berbeda dari sistem *grid computing*. Dalam jurnalnya, diusulkan klasifikasi dari komponen *grid computing* sesuai dengan mekanisme keamanan yang akan

diterapkan, yaitu: Resource level, Service level, Autentification & Authorization level, Information level dan Management level solution[2].

Sebelumnya, Anirban Chakraberti dkk. juga pernah mengusulkan klaisifkasi terhadap komponen dari *grid computing* ini terhadap mekanisme dan solusi keamanannya. Dalam usulannya dibagi 3 level yaitu, *Host level*, *Architecture level* dan *Credential level*. *Host level* membahas *host* (PC) yang terintegrasi dalam *grid computing* yang menjalankan kerja secara lokal dan *remote* dari *host* yang lain. Kerja secara lokal adalah bagian dari *host* tersebut sementara kerja secara *remote* adalah aktifitas berdasarkan perintah secara *remote* dari luar. Pada bagian ini permasalah keamanan yang timbul adalah ketika memeori dan *resource* CPU digunakan untuk kerja lokal dan *remote* berpeluang menghasilkan data yang *corrupt* dan kekurangan sumber daya pada *host*.

Architecture level ini berkaitan dengan arsitektur dari *grid computing* itu sendiri. Ada kekhawatiran bagaimana memetakan kebijakan yang berbeda pada seluruh bagian pada *grid*, kerena beragamnya *host* pembentuk *grid* dan harapan virtualisasi pada level pengguna. *Architecture level* ini juga membahas mengenai kemungkinan serangan *Denial Of Service* (DoS) pada sistem *grid*, serta sistem pengamanan informasi yang menjamin kerahasiaan, intgrasi dan model autentifikasi. *Credential level* adalah seusatu yang penting dalam *grid*, karena sistem yang diimplementasikan sangat bervariasi sehingga penting pengaturan akses terhadap *user* [3].

Dalam tulisan ini akan digunakan pendekatan yang pertama, karena merupakan model yang lebih baru dan banyak digunakan oleh perusahaan pengembang aplikasi keamanan dalam proses klasifikasi pengamanan dalam sistem *grid computing*. Tulisan ini merupakan survey terhadap perkembangan keamanan pada *grid computing* sesuai dengan level yang baik itu yang telah digunakan maupun masih dalam proses riset pengembangannya.



Gambar 1. Klasifikasi dari keamanan *grid computing*[2]

2. Keamanan pada Grid Computing

A. Bendahmane dkk. dalam tulisannya mengusulkan pembagian mekanisme dan solusi kemanan pada komponen yang berbeda dari sistem grid computing. Dalam jurnalnya, diusulkan klasifikasi dari komponen grid computing sesuai dengan mekanisme keamanan yang akan diterapkan, yaitu: Resource level, Service level, Autentification & Authorization level, Information level dan Management level solution[2].

a. Resource Level

Resource level ini fokus pada keamanan *node* (*hosts*) yang berada pada jaringan *grid computing* serta jaringan komunikasinya. *Host* yang terlibat dalam *grid computing* harus memiliki model manajeman keamanan yang baik untuk memastikan keamanan proses komputasinya. Juga untuk menjamin keamanan host itu sendiri sebagai sebuah personal desktop yang juga dimanfaatkan untuk hal lain oleh pemiliknya. Pada *resource level* ini juga dibahas solusi kemanan untuk jaringan komunikasi yang digunakan serta metode yang dapat digunakan untuk mendeteksi adanya sebuah serangan baik itu kepada *host* maupun kepada infrastruktur

jaringan komunikasinya.

b. Service level

Untuk *service* pada *grid computing* ancaman yang terjadi yaitu pada pelanggaran QoS akses service oleh yang tidak berhak dan *Denial Of Service* (DoS). DoS adalah ancaman yang paling serius dalam *grid computing*, karena selain dari eksternal, pengguna dari dalam sistem *grid* ini sendiri mungkin untuk melakukan serangan DoS. Sehingga diperlukan solusi keamanaan yang dapat mendeteksi dan mencegah serangan DoS ini.

c. Authentication dan authorization level

Pada bagian ini, ditentukan solusi keamanan untuk teknik *authentification* dan *authorization* pada *grid computing* terhadap akses penggunaan *resource* yang ada didalamnya. *Autentification* dilakukan untuk memastikan dan memverifikasi setiap *entity* didalam sebuah jaringan. *Authorization* adalah proses verifikasi dari sebuah aktifitas/aksi yang dapat dilakukan oleh *entity* setelah proses *authentication* sukses dilakukan.

d. Information level

Pada *information level* ini memastikan proses komunikasi antar dua buah *entity* berlangsung secara baik dan aman. Pada level ini memastikan proses pengiriman pesan dapat berlangsung secara rahasia, terjamin integritas data dan menjalankan *single sign on*.

e. Management level

Pada management level ini dibahas solusi kemanan dalam pengelolaan mandat dari setiap akses pada *grid computing*. Hal ini menjadi penting karena dalam *grid computing* terdapat banyak *entity*, komponen, pengguna dan kebijakan. Pengelolaan *management* ini sering disebut sebagai *Credential Management*, karena ada mandat yang bervariasi terhadap sebuah sistem dalam hal mengaksesnya.

3. Solusi Keamanan pada Grid Computing

A. Resource Level

1. Host Security

Sandboxing

Sandboxing dapat digunakan untuk mengisolasi *host* pada *grid computing* untuk menjamin penggunaan *resource* didalam *grid*. Dengan *sandboxing* ini dapat dilakukan pemisahan yang jelas untuk *resource* dari *host* yang digunakan untuk *grid* dan *resource* yang akan digunakan secara privat oleh pemilik desktop tersebut. Ada dua jenis dalam model *sandboxing* ini, yaitu :

User space sandboxing,

Virtual machine adalah salah satu dapat dibangun untuk proses *sandboxing*. Salah satu yang saat ini digunakan adalah *entropia virtual machine* (EVM)[4]. pada sistem ini, ada dua komponen tambahan penting dari desktop yang terlibat sebagai *host* pada *grid*, yaitu *desktop controler* dan *sandbox execution layer*. *Desktop controller* bertugas untuk mengeksekusi proses yang harus dijalankan pada desktop tersebut sebagai bagian dari *grid* sekaligus melakukan *monitoring* terhadap proses tersebut. Sementara *sandbox execution layer* melakukan semacam isolasi utnuk menjamin keamanan dan mengatur mekanisme *interface* pada desktop *controller*.

Application sandboxing

Pada *sandboxing* ini juga dikenal dengan *proof carrying code* (PCC) yang bekerja pada *aplication layer*. Dimana PCC ini digunakan untuk memastikan proses *running* dari *code* yang belum dipercaya. PCC ini memastikan bahwa *code* yang akan dieksekusi oleh pengguna berasal dari sumber yang tepat, sehingga tidak adanya eksekusi kode yang tidak sesuai[5].

Virtualisasi

Virtualisasi juga dapat dijadikan solusi keamanan pada

sebuah *host* dengan membangun sebuah *virtual machines* walau nantinya seolah-olah *host* tersebut merupakan sebuah *host* tunggal. Ada tiga model dalam pembangunan virtual *machines* ini, yaitu:

Host virtualization.Pada model ini, digunakan banyak sistem operasi yang berjalan pada sistem operasi utama. Tidak ada perubahan pada sistem operasi pertama, tetapi karena sistem operasi yang diinstal banyak memakan *resource* sistem operasi pertama, maka performa *host* pada model ini akan berkurang secara signifikan. Salah satu contoh model penggunaan *host virtualization* ini adalah Vmware GsX server. *Host virtualization* ini banyak digunakan karena mudah dalam pengoperasiannya dan memberikan solusi keamanan yang handal walau mengakibatkan pengurangan performa.

Para-Virtualization. Pada model ini dilakukan modifikasi pada sistem operasi utama dan dilakukan kompilasi ulang. Proses ini mengakibatkan berkurangnya *overhead* yang ditimbulkan dan lebih baik jika dibandingkan dengan model *hosted virtualization*. Contoh dari penggunaan para *virtualization* ini adalah Xen yang dikembangkan di Universitas Cambridge. Saat ini, karena sifatnya yang *open source* dan memiliki performa yang baik, xen sudah diimplementasikan secara komersil.

Shared Kernel. Contoh dari model *shared kernel* ini adalah *virtual server linux*. Dimana sistem menggunakan *kernel* bersama untuk aplikasi yang berbeda.

Solusi virtualisasi pada *host* ini menjadi pilihan yang cukup memberikan keamanan terhadap *host* pada *grid computing*. Tetapi harus diperhatikan akibat yang ditimbulkan dari penggunaan solusi ini, karena seperti pada *hosted virtualization* menyebabkan *overhead* yang tinggi dan menjadikan performa menjadi berkurang. Virtualisasi ini sangat cocok dikembangkan pada sistem yang *opensource* dan masih perlu sepakati kebijakan yng dapat diberlakukan secara umum tanpa terpengaruh sistem operasi apa yang akan digunakan pada tiap *host*.

Network security

VPN dan *firewall* banyak dikembangkan untuk keamanan jaringan komunikasi pada *grid computing*. Jaringan antara *host* dengan server, server dengan server, membutuhkan keamanan yang baik agar proses komputasi yang diharapkan dapat berjalan tanpa ada gangguan dari segi keamanan. Ada beberapa model yang telah dikembangkan saat ini, seperti *adaptive firewall grid* dan *hose service model*.

Adaptive Firewall Grid

AGF dikembangkan di Universitas Denmark (DTU). Seperti penggunaan *firewall* secara umum, AGF dikembangkan untuk memastikan setiap *port* yang akan digunakan dalam setiap *service* dari *grid computing* dan menentukan *range* dari setiap *port* untuk proses penerimaan informasi. AGF dikembangkan secara fleksibel dimana *port* akan dibuka dan ditutup sesuai dengan *service* yang dijalankan, sehingga pada satu proses *service port-port* yang dianggap tidak diperlukan dan berbahaya jika terbuka akan ditutup[6].

Hose service model

Hose service model ini dikembangkan oleh peneliti dari AT&T. seperti layanan VPN, *hose service model* ini menjadikan setiap jaringan seolah-olah memiliki kanal khusus dan akan dikumpulkan secara kontinu dalam proses komunikasinya. Sehingga setiap user mendapatkan informasi yang utuh untuk setiap informasi yang masuk dan keluar dari sumber yang berbeda didalam jaringan VPN tersebut.

Intrusion Detection System (IDS)

Penggunaan *grid computing* secara lebih luas saat ini mengakibatkan perlunya sebuah sistem yang dapat mendeteksi serangan baik terhadap infrastruktur jaringan maupun *host* yang berada pada jaringan tersbut. Ada dua model yang digunakan dalam

mendeteksi serangan, yaitu secara anomali dan menggunakan *signature*. Secara anomali, maka sistem akan mendeteksi serangan berdasarkan adanya ketidakbiasaan/abnormalitas dari model sistem yang dibangun terhadap kebiasaan yang seharusnya berlaku. Sehingga jika ada sebuah *service* yang diluar dari kebiasaan maka sistem akan menganggap itu adalah sebuah serangan. Selanjutnya berdasarkan *signature*, deteksi serangan dilakukan mendeteksi tanda dari serangan. Dalam hal ini model-model dari serangan pada system sudah dikenali oleh sistem tersebut perdasarkan pengamatan dan pengalaman. Berjalannya kedua sistem ini berdasarkan rekam jejak dari kebiasaan dari sistem dan kebijakan yang diterapkan padanya.

Contoh pengembangan dari *intrusion detection system* adalah SNORT. Sesuai dengan komponen dari IDS ini, SNORT berfungsi monitoring terhadap informasi yang diberikan oleh sensor yang telah dipasang pasa sistem *grid*, dimana sensor ini akan melakukan pengamatan dan mendeteksi serangan. SANTA-G adalah contoh dari sensor yang digunakan. Selanjutnya contoh lain dari IDS ini adalah GIDA, dan IACID dan Oracle 10G databese.

B. Service level

Denial of Service (DoS) adalah ancaman yang paling serius dalam grid computing, karena selain dari eksternal, pengguna dari dalam sistem grid ini sendiri mungkin untuk melakukan serangan DoS. Sehingga diperlukan solusi keamanaan yang dapat mendeteksi dan mencegah serangan DoS ini.

Seperti juga keamanan pada sistem lain, menghindari serangan DoS pada *grid computing* terdiri dari dua buah solusi yaitu preventive dan reaktif[5].

Preventif adalah pencegahan serangan seperti *filtering* (paket dan aplikasi), penyembunyian lokasi dan pengaturan kapasistas jaringan. Untuk *filtering* saat ini sudah dikembangkan DPF (*distributed packet filtering*), dimana *packet* akan diterima atau dibuang berdasaran *interface* dari penerima paket tersebut. Sementara untuk solusi yang reaktif adalah kemampuan sistem

untuk melakukan deteksi serangan setelah serangan selesai terjadi. Solusi saat inii yang digunakan adalah *link testing*, *logging*, ICMP *traceback* dan IP *traceback*.

Dua model pendekatan ini, prefentive dan reaktif, memiliki keunggulan dan kelemahan masing-masing yang secara umum mempengaruhi tingkatan solusi keamanan dari *service level* itu sendiri. Sementara DoS sampai saat ini belum memungkinkan untuk dicegah dan mendeteksinya dengan sebuah solusi saja. Saat ini, pedekatan preventif saja yang sudah dapat diimplementasikan dengan baik, karena pada pendekatan reaktif, seperti ICMP *traceback* itu, malah mengakibatkan DoS itu sendiri secara tidak langsung.

C. Authentication dan authorization level

1. *Authentication*

Authentication dilakukan untuk memastikan dan memverifikasi setiap *entity* didalam sebuah jaringan. Globus telah mengaplikasikan *Grid Security Infrastructure* (GSI) untuk proses verifikasi setiap *entity* didalam jaringan baik itu pengguna, sumber daya maupun *service* yang merupakan bagian dari *grid computing* itu sendiri. Kemampuan verifikasi *entity* pada GSI ini berbasis pada X.509 *certificate*. Proses *authentication* dengan X.509 *certificate* ini memiliki kemampuan yang handal, tetapi memerlukan *public-key infrastucture* dalam prosesnya, dimana ini akan berpengaruh kepada skalabilitas dari sistem tersebut. Kendala lain adalah GSI ini tidak mendukung kemampuan interaksi dengan sistem *authetication* lain seperti Karberos, sehingga dibutuhkan poses konversi seperti yang dilakukan oleh KX.509/KCA (*Karberos Certificate Authority*) pada GSI ke *Karberos Gateway* dan SSLK5/ PKINIT pada Karberos ke GSI *gateway*[5].

Model *authentication* lain yang dapat diterapkan pada *grid computing* adalah LDAP. LDAP dapat digunakan sebagai *identity management* dan *monitoring*. Beberapa standar LDAP dapat digunakan pada *grid computing* seperti (*login/password, password with hasing password with ssl, dan X.509 certificate*).

2. *Authorization*

Authorization adalah proses verifikasi dari sebuah aktifitas/ aksi yang dapat dilakaukan oleh *entity* setelah proses *authentication* sukses dilakukan. ada dua sistem *authorization* yang diterapkan dalam *grid computing* yaitu secara terpusat seperti CAS, VOMS, dan secara lokal seperti Akenti, PERMIS, Grid-MAP.

Authorization secara terpusat ini adalah sebuah poses *authorization* seluruh bagian dari *virtual organisation* (VO) pada *grid computing*. VO ini mengumpulkan penggguna yang tersebar dan *resource provider* (RP) yaitu pembagi dari beberapa administrator yang menerapkan kebijakan berbeda. RP memberikan hak kepada VO untuk mengijinkan user mengakses sumber daya yang ada padanya sesuai dengan informasi yang telah diberikan sebelumnya oleh RP kepada VO. Tetapi pada akhirnya keputusan boleh tidaknya *use*r mengakses *resource* tetap berada pada *resource* tersebut.

Sementara *authorization* secara lokal, setelah proses pembangunan hubungan antar *community* terjadi, RP memberikan hak kepada setiap *user* untuk mengakses *resource* yang ada padanya, tetapi keputusan boleh tidaknya *user* mengakses berada pada RP tersebut.

Dari dua model proses *authorization* ini ada masing-masing memiliki kelebihan dan kekurangan. Secara skalabilitas, administrator memiliki kemampuan lebih jika proses *authorization* dilakukan secara terpusat. Sementara dari segi keamanan penggunaan sertifikat (terpusat) dalam proses *authorization* menjadi pilihan yang cukup menjanjikan karena kemampuannya menerapkan penggunaan *username* dan *password*. Dalam hal menjaga sistem tetap dalam kendali yang sah, walau sudah dikuasai oleh penyerang, maka sistem lokal memiliki kemampuan lebih. Karena pada sistem yang terpusat, VO tidak memiliki kebijkan mengambil alih *resource* yang sudah dikuasai oleh *user* yang tidak berhak.

D. Information level

Ada dua pendekatan proses pada level ini, yaitu *security* pada *transport layer* dan/atau *security* pada *message layer*.

Keamanan pada *transport layer* menjaga data yang ditransfer pada *layer transport* dengan menggunakan standar seperti *transport layer security* (TLDS). GT4 menjadikan TLS/SSL sebagai *default* dari keamanan pada layer transport ini. Sementara *message layer security* bekerja pada layer diatasnya dan menggunakan *standard web service* seperti WS-Security[5]. Penggunaan *message layer security* ini adalah sebagai alternatif dari SSL karena kemampuanya yang handal dan lebih cepat dibandingkan *security* pada *message level*. Penggunaan *security* pada *message level* baru diterapkan jika ada kebutuhan khusus.

E. Management level

Kebutuhan pada *management level* ini adalah proses inisiasi, dimana hak akses dari sebuah *entitiy* terdapat sistem berasal dari proses inisiasi ini. sehingga administrator tidak terlalu susah untuk secara aktif memantau aktifitas pada sistem. *Credential Management* (CM) *system* dapat dibagi menjadi dua kategori, yaitu *credential repositories system* dan *credential federation system*. *Credential repositories* atau juga disebut *credential storage system* adalah dengan cara memberikan tanggungjawab dari *user* kepada sistem untuk memiliki mandat penyimpanan *credential storage*. Beberapa contoh solusi yang saat ini banyak digunakan untuk *credential storage system* adalah *smart cards*, *virtual smart cards* dan *MyProxy Obline Credential Repositories*. *Smart cards* adalah seperti *token* kartu kredit yang menyimpan *secret keys* dari *user*. Ini adalah solusi yang baik untuk tingkat kemanan yang tinggi, tapi penggunaan *smart cards* ini memerlukan biaya yang tinggi. *Virtual Smart cards* mirip seperti *smart cards* tetapi berbentuk *software*. *MyProxy online credential* manager adalah salah satu pengembangan dari penelitian virtual *smart cards* yang banyak digunakan dalam *credential repositories* di *grid computing*.

Credential federation system atau disebut juga *credential*

share system merupakan *system*, standar dan protokol yang digunakan proses berpindah dari satu *system* domain atau realms ke yang lainnya. Bentuk solusi keamanan pada *credential federation system* ini adalah Liberty Project, KX.509, dan VCMan.

Dalam *Management level* ini juga diberi solusi keamanan untuk menjaga kepercayaan. Ada dua model untu menjaga kepercayaan sistem terhadap *entity* yang berada didalamnya. Yang pertama adalah berdasarkan kepada reputasi seperti solusi yang ditawarkan oleh *PeerTrust*, *XenoTrust* dan NICE. Yang kedua adalah berdasarkan kebijakan, contoh dari solusi *trust management model* ini adalah *TrustBuilder*.

4. Kesimpulan

Grid Computing adalah salah bidang kajian yang sampai dengan saat ini masih menjadi isu yang hangat, termasuk dalam hal keamanan. Ada tiga tantangan dalam hal keamanan pada *grid computing* ini, yaitu integrasi dengan sistem yang sudah ada, interopabilitas antar sistem pada lingkungan sistem yang berbeda serta kepercayaan antar domain dari setiap sistem. Dengan pengklasifikasian setiap level pada *grid computing* yang telah diusulkan ini, akan lebih mudah bagi para peneliti untuk mengembangkan dan memprtajam solusi keamanan dari setiap levelnya. Yang masih sering menjadi permasalahan dengan perkembangan *grid computing* adalah semakin meluas penggunaannya, interopabilitas antar lingkungan sistem merupakan ancaman yang paling tinggi. Karena dengan interopabilitas sistem yang meningkat juga akan meningkatkan serangan. Sehingga masih perlu dikembangkan sistem keamanan pada *grid computing* yang kuat dan dapat bekerja pada lingkungan sistem yang beragam.

DAFTAR PUSTAKA

[1.] Foster and C. Kasselman, "The Grid 2: Blueprint for anew Computing Infrastructure," Morgan Kaufman, 2004.

[2.] A. Bendahmane, M. Essaidi, A. E. Moussaoui, A. Younes, "Grid Computing Security Mechanism: State-of-The-Art," IEEE, 2009.

[3.] A. Chakrabarti, A. Damodaran, S. Sengupta, "Grid Computing Security A Taxonomy," IEEE Computer Society, 2007.

[4.] E.Cody, R.Sharman, R.H.Rao, S.Upadhyaya, "Security in grid computing: A review and synthesis," Decision Support Systems 44 (2008) 749-764.

[5.] A.Chakrabarti. Grid Computing Security, Springer Berlin Heidelberg New York, 2007.

[6.] T.D. Yao. Adaptive Firewalls for the Grid. Master's Thesis, Technical University of Denmark, 2005.