Pemanfaatan Analisis dan Visualisasi Graf dalam Keamanan Siber

Florencia Wijaya 13518020[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13518020@std.stei.itb.ac.id

***Abstrak*—Beberapa tahun ini, aktivitas *hacking* dan serangan siber lainnya telah menjadi salah satu masalah yang cukup besar dalam bidang teknologi yang berkaitan dengan data. Isu ini membuat keamanan siber menjadi salah satu aspek yang penting. Banyak tim keamanan siber yang harus meningkatkan kinerjanya dalam menghadapi ancaman yang makin meningkat ini. Analisis dan visualisasi graf dapat digunakan untuk meningkatkan keamanan siber. Basis data bermodelkan graf bisa dimanfaatkan untuk menyimpan dan mengolah data dalam jumlah besar dan visualisasinya membantu dalam menganalisis ancaman siber secara lebih cepat.**

***Kata Kunci*—Graf , Keamanan Siber, Serangan Siber, Struktur Data**

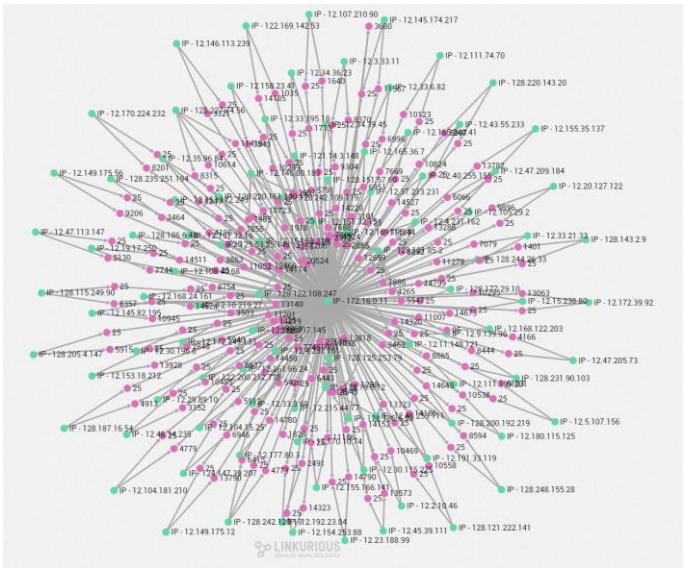
I. PENDAHULUAN

Selama beberapa tahun ke belakang ini, telah berkembang begitu banyak ancaman yang menyerang dunia siber. Ancaman-ancaman yang biasa disebut *cyber threats* (serangan siber) ini memiliki banyak bentuk, antara lain *malware*, *phishing*, *spear phishing*, *trojans*, *ransomware*, *denial of service*, dan *data breaches*. Efek dari serangan ini sangatlah berbahaya. Serangan ini dapat mencuri data seseorang secara digital dan mengeksposnya atau memeras si pemilik data. Serangan ini juga dapat membahayakan ketahanan nasional, contohnya menyebabkan kerusakan listik nasional, kerusakan pada alat-alat militer, dan mengakses dokumen-dokumen yang merupakan rahasia negara.

Adanya ancaman-ancaman seperti ini, tentu saja membuat orang-orang ingin menjaga data pribadi yang termasuk privasinya. Para pengusaha tentu ingin melindungi data sensitive perusahaannya. Semakin hari, pelaku penyerangan ini makin kreatif dan berinovasi, sementara metode dan alat yang ada untuk mengatasinya berkembang dengan lambat. Oleh karena itulah, dibutuhkan sebuah sistem keamanan siber (*cyber security*) yang dapat lebih efektif dalam mengatasi ancaman-ancaman ini.

Keamanan siber adalah sebuah usaha untuk melindungi sistem, jaringan, dan program dari serangan-serangan digital. Keamanan siber ini biasanya memiliki banyak lapisan proteksi yang tersebar di computer, jaringan, program, ataupun data yang ingin dijaga oleh seseorang. Dengan adanya keamanan siber, Internet menjadi suatu tempat yan lebih aman bagi semua orang.

Berbagai perusahaan atau suatu organisasi memiliki informasi dan jejak digital dari sistem yang mereka miliki. Banyak perusahaan atau organisasi besar mengolah jutaan data tiap harinya. Data yang ada ini dapat dikategorikan sebagai *big data*. Di sinilah masalah datang. Volume data yang sebesar ini (*big data*) tidak dapat dikelola oleh aplikasi *Security Information and Event Management* (SIEM) tradisional. Memang masalah ini tidak terlalu besar, tetapi ahli keamanan siber akan menemui beberapa kendala, seperti kesulitan untuk mengintegrasikan sumber baru, kompleksitas dalam struktur dan *query* data yang ada, dan performa yang buruk saat *querying* data. Maka dari itu, diperlukan suatu solusi lain untuk mengelola *big data* ini agar dapat mengatasi ancaman siber yang ada. Jawabannya adalah dengan menggunakan basis data yang memiliki representasi graf.



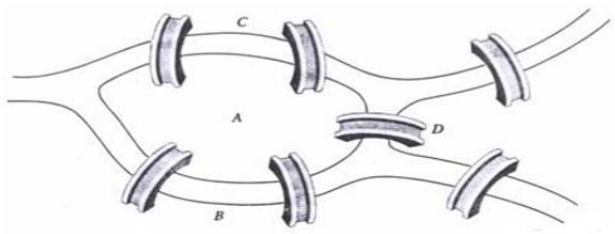
Gambar 1. Contoh Representasi Graf dalam Menganalisis Serangan Siber.
(Sumber : https://linkurio.us/blog/graph-data-visualisation-cyber-security-threats-analysis/)

Dengan representasi graf, data seperti catatan alamat IP, nama *server*, *registar*, catatan jaringan, dan catatan komunikasi, akan divisualisasikan dengan graf. Bukan hanya entitasnya, tetapi juga hubungannya satu sama lain. Cara mempresentasikan data dalam model graf seperti ini dapat membuat pekerja keamanan siber lebih cepat dan mudah dalam menginterpretasi data yang ada.

II. Dasar Teori

A. Graf

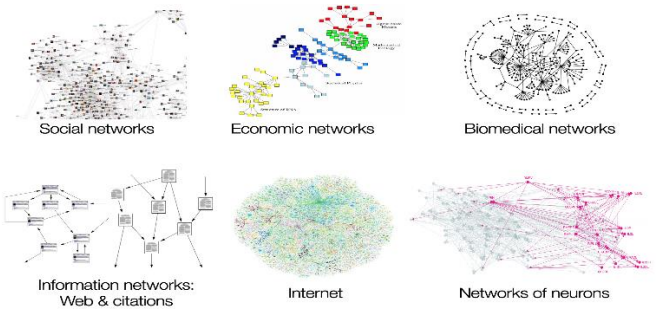
Graf mulai dikenal saat Leonhard Euler berhasil memecahkan Misteri Jembatan Koningsberg pada tahun 1736.



Gambar 2. Misteri Jembatan Koningsberg
(Sumber : staff.ayu_ws.gunadarma.ac.id)

Pada persoalan ini, daratan dinyatakan dengan simpul, sementara jembatan dinyatakan dengan sisi.

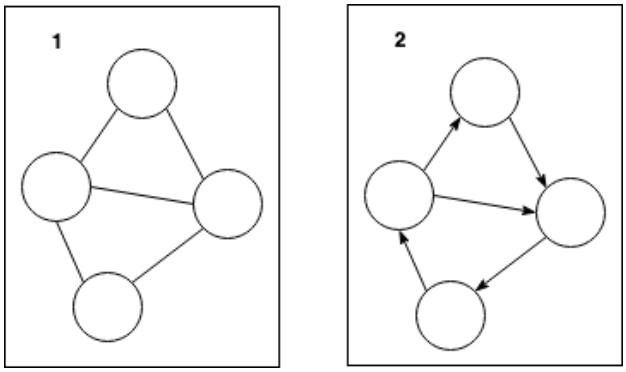
Graf dapat merepresentasikan begitu banyak pemodelan yang kompleks, seperti jaringan sosial, interaksi antarprotein, graf pengetahuan, kutipan, ataupun Internet. Berikut adalah contoh beberapa graf yang telah disebutkan.



Gambar 3. Contoh Pemanfaatan Graf dalam Berbagai Bidang
(Sumber : https://towardsdatascience.com/graph-theory-132122ac38f2)

Graf sendiri memiliki pengertian berupa struktur data yang terdiri atas simpul (*vertice*/V) dan sisi (*edge*/E). Graf memiliki notasi G(V,E). Simpul dapat menggambarkan peluang ataupun variabel acak. Sisi juga dapat diberikan nilai. Graf umumnya dimanfaatkan untuk merepresentasikan objek-objek diskrit dan hubungan antarobjek tersebut. Graf sendiri memiliki tujuan sebagai visualisasi objek.

Berdasarkan arahnya, graf dapat dibedakan menjadi dua jenis, yaitu graf berarah (*directed graph*) dan graf tidak berarah (*undirected graph*). Graf berarah adalah graf yang sisinya memiliki arah, sementara graf tidak berarah adalah graf yang sisinya tidak memiliki arah.



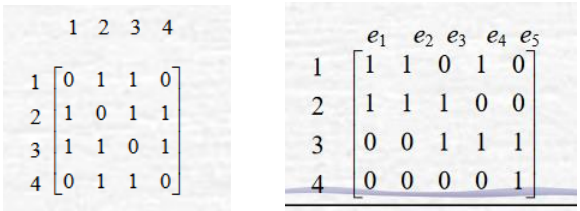
Gambar 4. Graf Berarah dan Graf Tidak Berarah
(Sumber : https://towardsdatascience.com/graph-theory-132122ac38f2)

Berdasarkan ada tidaknya gelang atau sisi ganda pada graf, graf dapat dibedakan menjadi dua jenis, yaitu graf sederhana (*simple graph*) dan graf tak sederhana (*unsimple graph*). Graf sederhana adalah graf yang tidak mengandung gelang, sementara graf tak sederhana adalah graf yang mengandung gelang.

Ada pula yang disebut sebagai derajat graf. Derajat pada graf berarti jumlah dari derajat simpul-simpulnya. Derajat simpul itu sendiri berarti banyaknya sisi yang terhubung dengan simpul itu sendiri. Ada suatu teorema yang menyatakan bahwa jumlah derajat semua simpul pada suatu graf adalah dua kali banyaknya sisi pada graf. Simpul yang memiliki suatu gelang dihitung telah memiliki derajat 2. Derajat total suatu graf selalulah genap. Dalam sembarang graf, jumlah simpul yang berderajat genap selalu genap. Genap-ganjilnya derajat simpullah yang menentukan apakah suatu simpul dapat disebut genap atau ganjil.

Ada beberapa terminologi lain dalam graf. Pertama, ketetanggaan. Dua buah simpul dikatakan terhubung apabila terdapat sisi yang menghubungkan kedua sisi tersebut. Kedua, bersisian. Sebuah sisi dikatakan bersisian dengan sebuah simpul jika ia menghubungkan simpul tersebut dengan suatu simpul lainnya. Ketiga, ada istilah lintasan dan sirkuit. Lintasan adalah sebuah barisan simpul dan sisi untuk menghubungkan simpul awal dan simpul tujuan. Sirkuit adalah sebuah lintasan tertutup, yang berarti lintasan tersebut bermula dan berakhir pada simpul yang sama. Jika terdapat lintasan dari suatu simpul ke simpul lainnya, maka kedua simpul tersebut disebut terhubung. Keempat, subgraf. Subgraf adalah bagian lebih kecil dari graf. Sebuah subgraf G_1dapat dikatakan bagian dari graf G jika simpul dan sisi dari G_1 merupakan anggota dari himpunan simpul dan sisi G.

Ketetanggaan dan kebersisian dalam graf dapat direpresentasikan dalam bentuk matriks.



Gambar 5. Matriks Ketetanggaan dan Matriks Kebersisian

(Sumber : http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2015-2016/Graf%20(2015).pdf)

Pada matriks ketetanggaan, baris dan kolom menunjukkan urutan simpul-simpul. Jika elemen matriksnya 1, berarti terdapat sisi antara simpul baris dan kolom (bertetangga). Jika elemen matriksnya 0, berarti tidak terdapat sisi antara simpul baris dan kolom. Sementara itu, pada matriks bersisian, barisnya menunjukkan simpul, sedangkan kolomnya menunjukkan sisi. Jika elemen matriksnya 1, berarti simpul baris tersebut bersisian dengan sisi kolom tersebut (bersisian). Jika elemen matriksnya 0, berarti simpul baris tersebut tidak bersisian dengan sisi kolom tersebut.

B. Serangan Siber

Dikutip dari https://dspace.uii.ac.id, serangan siber (*cyber crime*/*cyber threat*) adalah sebuah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan computer menjadi alat, sasaran atau tempat terjadinya kejahatan termasuk ke dalam kejahatan dunia maya antara lain penipuan lelang secara *online*, pemalsuan cek, penipuan kartu kredit, *confidence fraud*, penipuan identitas, pornografi anak. Menurut Brenda Nawawi (2001), serangan siber ini adalah bentuk fenomena baru dalam dunia kejahatan sebagai akibat dari perkembangan teknologi informasi.

Ada sepuluh tipe umum dalam serangan siber.

1. *Malware*. Serangan ini menjalankan serangan yang merusak pada target, seperti merusak data atau mengambil alih sistem.
2. *Phising*. Serangan ini dijalankan melalui surat elektronik (*e-mail*) yang mengelabui penerima untuk membongkar data pribadinya. Berdasarkan https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/, disebutkan bahwa terdapat tiga entitas yang biasanya ada di serangan berjenis *phising*.
   a. Alamat IP. Alamat IP adalah suatu label numerik yang terhubung dengan perangkat yang berada di dalam suatu jaringan komputer yang menggunakan *Internet Protocol* untuk berkomunikasi.
   b. *Name server*. Entitas ini memiliki arti sebagai perangkat komputer yang menyediakan jaringan untuk mengubah nama *domain* menjadi alamat IP.
   c. *Register*. *Register* adalah entitas yang mengatur ‘pemesanan’ nama *domain* yang ada di Internet.
3. *Spear Phising*. Serangan ini adalah peningkatan dari *phising*, dimana penyerangnya dapat berpura-pura menjadi orang yang dikenal penerima surat elektronik.
4. “*Man in The Middle*”. Serangan ini membuat penyerang dapat “mencegat” surat elektronik antara dua orang dan mengganti pesan mereka.
5. *Trojans*. Serangan ini adalah *malware* yang menyamar di dalam suatu sistem, lalu melepaskan kode yang merusak.
6. *Ransomware*. Serangan ini melibatkan data yang terenkripsi ke sistem yang ditargetkan dan meminta *ransom* (pemerasan).
7. *Denial of Service*. Penyerang mengambil alih banyak perangkat.
8. *Attacks on IoT Device*. Penyerang mengambil alih banyak perangkat IoT yang rentan terhadap serangan siber.
9. *Data Breaches*. Serangan ini berupa pencurian data.
10. *Malware on Mobile Apps*. Perangkat *mobile* rentan terhadap serangan siber. Penyerang dapat menanamkan *malware* pada suatu aplikasi.

C. Keamanan Siber

Dikutip dari http://www.phintraco.com/pentingnya-cyber-security/, keamanan siber (*cyber security*) adalah teknologi, proses, dan praktik yang dirancang untuk melindungi jaringan, computer, program, dan data dari serangan, kerusakan atau akses yang tidak sah. Keamanan siber dapat juga diartikan sebagai cara untuk melindungi informasi yang ada dari serangan siber. Keamanan siber ini bermanfaat untuk menjaga sistem dari serangan siber, seperti mencegah penyalahgunaan akses maupun pemanfaatan data oleh seseorang yang tidak memiliki akses ke data tersebut.

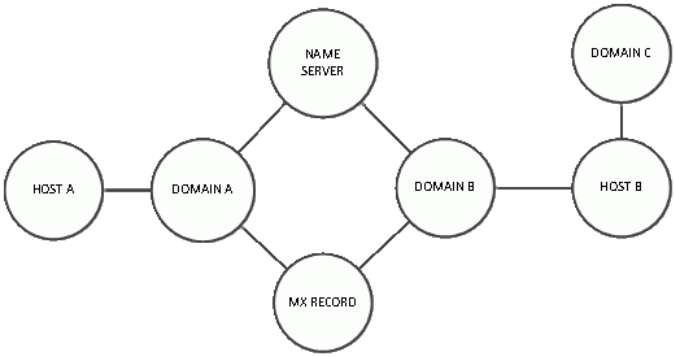
Ada beberapa elemen pada keamanan siber.

1. Dokumen *security policy*. Semua proses terkait keamanan informasi dijalankan dalam dokumen ini, sehingga dokumen ini menjadi dokumen standar yang dijadikan acuan dalam keamanan siber.
2. *Information infrastructure*. Hal ini merupakan media yang berperan dalam kelangsungan operasi informasi, termasuk *hardware* dan *software*.
3. *Perimeter defense*. Ini adalah media yang menjadi pertahanan pada infrastruktur informasi yang ada. Bentuk dari *perimeter defense* adalah IDS, IPS, dan *firewall*.
4. *Network Monitoring System*. Ini adalah media yang berfungsi untuk memonitor kelayakan, utilisasi, dan performa dari infrastruktur informasi.
5. *System Information and Event Management*. Ini adalah media yang berperan dalam mengawasi berbagai kejadian yang ada pada jaringan, termasuk kejadian-kejadian yang melibatkan serangan siber.
6. *Network Security Assessment*. Ini adalah media yang berperan sebagai mekanisme control dan mengukur level dari suatu keamanan informasi.
7. *Human Resource and Security Awareness*. Elemen ini berkaitan dengan sumber daya manusia dan kesadaran manusia terhadap pentingnya keamanan informasi.

III. Aplikasi Graf dalam Keamanan Siber

Tim keamanan siber dalam suatu perusahaan atau organisasi mempunyai begitu banyak data, antara lain catatan IP, catatan jaringan, catatan komunikasi atau *server*. Data ini diperoleh dari alat-alat yang digunakan untuk mengawasi sistem mereka. Data ini kebanyakan tidak terstruktur karena sumber data yang tercampur-aduk dan tidak lengkap. Namun, volume data yang besar menjadi sebuah halangan bagi *tools* tradisional yang tidak diciptakan untuk mengolah data dalam jumlah besar (*big data*). Data tidak terstruktur yang disusun di sebuah visualisasi bersifat *table-oriented* tentunya akan membawa kesulitan. Oleh karena itu, dapat digantikan dengan basis data berbasiskan graf yang bisa memberikan kemudahan dalam menyimpan dan mengolah data, walaupun volume datanya terus berkembang.

Di sinilah pemodelan dengan representasi graf dimulai. Data yang ada, seperti *domain* dan alamat IP direpresentasikan sebagai simpul di dalam graf. Lalu, hubungan antardata tersebut direpresentasikan oleh sisi yang menghubungkan dua simpul tertentu. Jadi, jika ada dua simpul yang bertetanggaan, berarti dua data tersebut memiliki kaitan.



Gambar 6. Data dalam model graf
(Sumber : https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/)

Melalui pemodelan seperti ini, data dapat diinterpretasikan dengan cepat. Semua data yang ada direpresentasikan dalam simpul dan jika data tersebut ada yang memiliki hubungan, maka akan ditambahkan sisi. Simpul-simpul yang bertetangga berarti memiliki hubungan. Atau dengan kata lain, sisi yang bersisian dengan dua simpul tertentu, berarti dua simpul tersebut memiliki hubungan. Jika terdapat lintasan antara suatu simpul dengan suatu simpul lainnya, maka simpul tersebut saling terhubung. Berdasarkan contoh graf di atas, *domain* A dan *domain* B terhubung karena terdapat lintasan dari *domain* A ke *domain* B. Lintasan tersebut terbentuk karena *domain* A dan *domain* B berbagi *name server* dan MX *record* yang sama, walaupun *domain* A dan *domain* B memiliki *host* yang berbeda. *Domain* C terhubung dengan *domain* B karena terdapat lintasan dari *domain* C ke *domain* B. Lintasan tersebut ada karena *domain* B dan *domain* C memiliki *host* yang sama. Namun, *domain* C tidak memiliki hubungan langsung dengan *domain* A.

Ada beberapa perusahaan keamanan siber yang telah menerapkan analisis dan visualisasi basis data berbasiskan graf untuk menganalisis serangan siber. Contohnya adalah Cisco, sebuah perusahaan keamanan siber. Cisco memiliki 25 hingga 30 juta data *domain* yang ada di Internet dan mengetahui mana *domain* yang dikendalikan oleh peretas. Membuat sebuah *list* yang berisi kumpulan *domain* yang dikendalikan oleh peretas untuk menghindari ancaman siber yang berpotensi dari *domain* tersebut adalah langkah yang strategis. Namun, masih ada 180 juta *domain* lainnya yang belum diketahui oleh Cisco. Jika terjadi serangan siber, maka Cisco akan segera menganalisis data yang ada untuk mencari koneksi dari data yang ada di *database* dengan *domain* yang baru saja digunakan untuk menyerang. Biasanya, *domain-domain* yang ada saling berkaitan.

Di sinilah menganalisis sebuah basis data yang berbentuk graf sangat membantu, yaitu dalam mencari koneksi antardata dalam suatu basis data yang besar. Dengan analisis graf, Cisco mampu menggunakan *domain-domain* penyerang tadi untuk menemukan serangkaian *domain* mencurigakan lainnya yang merupakan bagian dari 180 juta *domain* yang belum teridentifikasi. Jika ada yang simpul yang bertetangga ataupun jika ada keterhubungan antara dua simpul, maka *domain* tersebut dapat langsung dikualifikasikan sebagai *domain* yang mencurigakan, walaupun memang belum pernah digunakan.

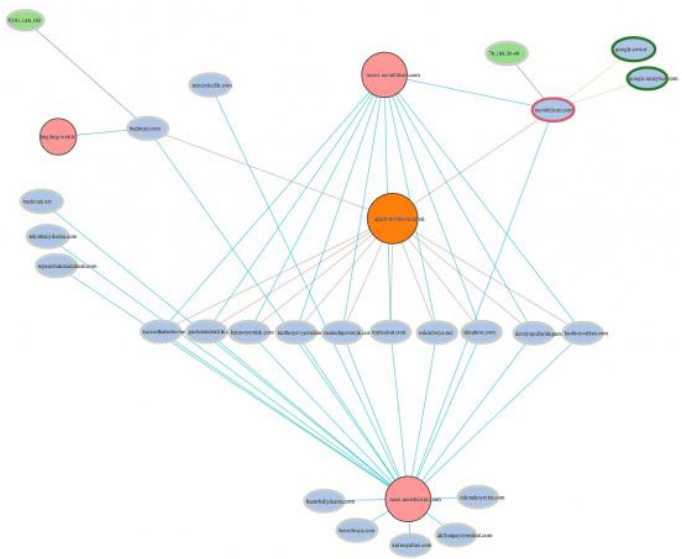
Teknologi graf seperti Neo4j, GraphLab, dan Titan dapat membantu dalam menganalisis graf secara cepat. Berikut adalah *query* yang ditulis dengan *Cypher the* Neo4j.

```
MATCH (baddomain:Domain_name)-[r*2]-(suspiciousdomains:Domain_name)
WHERE baddomain.reputation = 'Very negative reputation'
RETURN DISTINCT suspiciousdomains
```

Gambar 7. Query dalam Cypher the Neo4j
(Sumber : https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/)

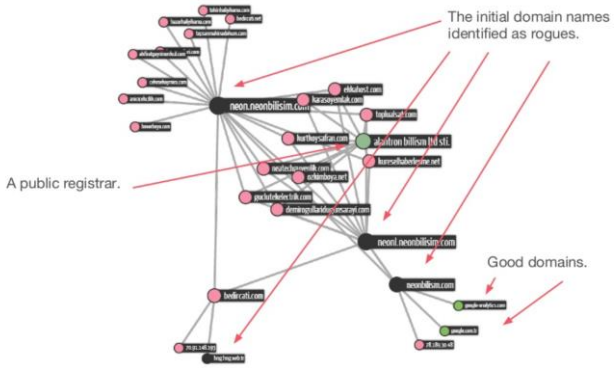
Query ini digunakan untuk memperoleh semua *domain* yang memiliki hubungan dengan penyerang siber. Terdapat 25 hasil.

Selain analisis graf, juga diperlukan sebuah visualisasi. Visualisasi graf membantu manusia dalam memahami data yang ada dan memberikan *insight* kepada manusia untuk mengambil keputusan yang tepat. Dari sini, analis dapat mencoba mengerti dan menginterpretasikan data yang terhubung dan menyelidiki hal-hal aneh yang terjadi pada jaringan. Presisi tinggi yang dihasilkan oleh visualisasi graf bisa membantu analis untuk mengerti aktivitas-aktivitas yang berkaitan dengan keamanan secara cepat. Selain itu, dengan adanya visualisasi, penggambaran ini dapat mengurangi skala dan kompleksitas dari analisis yang harus dilakukan oleh program.



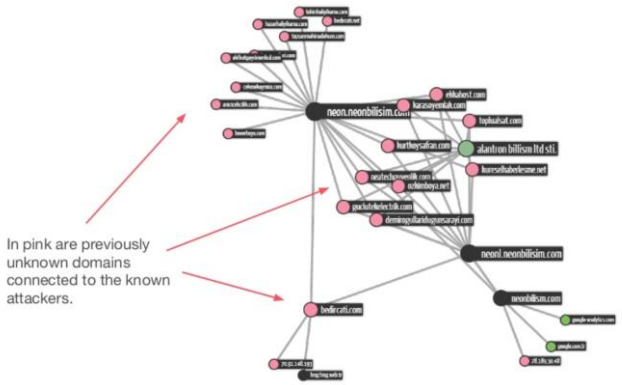
Gambar 8. Contoh Graf yang Memuat Informasi Entitas yang Terlibat dalam Sebuah Serangan Siber
(Sumber : https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/)

Dalam visualisasi graf, cara pertama untuk mencari semua *domain* yang berkaitan dengan penyerang adalah dengan terlebih dahulu mengidentifikasi penyerang tersebut.



Gambar 9. Mengidentifikasi Penyerang dalam Pemodelan Graf
(Sumber : https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/)

Setelah berhasil mengidentifikasi semua *domain* yang digunakan penyerang, cara kedua adalah mengidentifikasi semua *domain* yang terkait atau terhubung dengan penyerang tersebut. Untuk mencari keterkaitan atau keterhubungan ini, seperti yang telah dijelaskan, apabila terdapat sisi yang menghubungkan dua simpul tertentu, maka dapat dikatakan bahwa kedua simpul tersebut memiliki hubungan. Nama *domain* yang mencurigakan dapat diawasi sehingga *domain* tersebut tidak bisa digunakan lagi dalam serangan lainnya. Lalu, dari koneksi yang ada, nama-nama *domain* yang mencurigakan dan yang berada dalam kendali peretas bisa langsung diblok sehingga tidak dapat digunakan sama sekali oleh peretas.

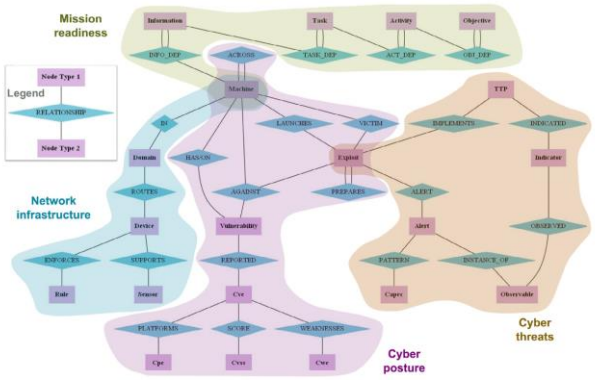


Gambar 10. Mencari Koneksi AntarSimpul dalam Pemodelan Graf
(Sumber : https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/)

Semua informasi ini memang dapat disajikan dalam bentuk tabel ataupun list, tetapi analis akan menemui kesulitan untuk menemukan koneksi antardata tanpa visualisasi graf. Namun, saat berurusan dengan data yang begitu banyak, visualisasi secara keseluruhan akan cukup menyulitkan karena ada begitu banyak informasi. Oleh karena itu, analis bisa cukup hanya dengan melihat subgraf spesifik yang lebih kecil atau graf dalam skala yang lebih kecil.

Analisis dan visualisasi graf ini juga telah dimanfaatkan oleh *CyGraph*, sebuah sistem untuk meningkatkan keamanan jaringan. Sistem ini juga memanfaatkan graf dalam keamanan siber. Tujuan dari *CyGraph* adalah memaksimalkan kemampuan untuk menemukan ancaman yang berpotensi terjadi di masa depan dalam waktu yang paling minimum untuk menyusun dan menyimpan data yang terpisah-pisah menjadi memiliki sebuah hubungan.

Dalam *https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf*), dijelaskan bahwa *CyGraph* membuat graf yang menampilkan potensi serangan dalam suatu jaringan. Hampir sama dengan Cisco, *CyGraph* mengumpulkan semua data, termasuk *network topology*, *firewall rules*, *host configurations*, dan *vulnerabilities*. Graf ini akan terus berkembang dan bertambah seiring dengan penambahan data yang ada sehingga dapat memberikan respon yang tepat jika terdapat serangan. Dengan pemodelan graf, *CyGraph* juga menyediakan bahasa *query* yang spesifik ke suatu *domain*. *CyGraph* dapat memetakan serangan yang sekiranya mampu dilakukan oleh seorang peretas dan menggabungkan seluruh peringatan yang ada. Berikut adalah contoh model graf 'pengetahuan' dari CyQL (seperti basis data dalam bentuk graf) yang berisi informasi data yang telah dikumpulkan oleh *CyGraph* (*network topology*, *firewall rules*, *host configurations*, dan *vulnerabilities*) dan serangan-serangan yang terjadi serta peringatan yang ada.



Gambar 11. Graf Pengetahuan atau Basis Data dalam Graf
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

Berikut adalah *grammar* yang dipakai untuk versi prototipe dari CyQL.

```
grammar CyQL;
@header {
    package org.mitre.cygraph.dsl;
}

query : subset (SETOP subset)* EOF ;
subset : call
           | '(' subset (SETOP subset)* ')' ;
call : FUNCTION '(' ')'
     | FUNCTION '(' paramList ')' ;

paramList : param (',' param)* ;
param : ID '=' disjunction
      | ID '=' value
      | ID '=' valueList ;

valueList : '[' value (',' value)* ']' ;
value : ID
      | INT
      | GLOB
      | STRING
      | IPV4
      | ipv4Range ;

disjunction : conjunction ('or' conjunction)* ;
conjunction : specifier ('and' specifier)* ;
specifier : '{' paramList '}'
          | '(' disjunction ')' ;

ipv4Range : IPV4 '-' IPV4
          | IPV4 '/' IPV4
          | IPV4 '/' INT ;

IPV4 : INT '.' INT '.' INT '.' INT ;
```

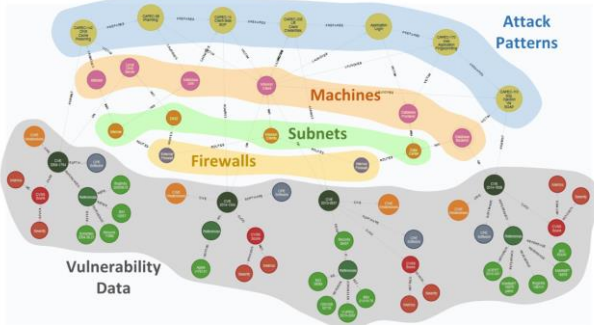
Gambar 12. *Grammar* dalam CyQL.
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

```
FUNCTION : 'network' | 'all' |
'exploitPaths' | 'correlateAlerts' |
'cveData' ;
SETOP : 'join' | 'except' | 'union' |
'intersect' ;
ID : [a-z][a-zA-Z0-9]* ;
GLOB : [a-zA-Z*][a-zA-Z0-9*_-]* ;
INT : [0-9]+ ;

STRING : '"'
            (   ESC
                |   ~('"'|'\\')
                )*
            '"' {
                setText(

org.antlr.v4.misc.CharSupport
.getStringFromGrammarStringLiteral(
   getText())
   );
}
;

fragment ESC :   '\\' (["\\/bfnrt] |
UNICODE) ;
fragment UNICODE : 'u' HEX HEX HEX HEX;
fragment HEX : [0-9a-fA-F];

COMMENT : '//' ~[\n]* '\n' -> skip;

BLOCK_COMMENT : '/*' .*? '*/' -> skip;
WS : [ \t\r\n]+ -> skip ;
```

Gambar 13. *Grammar* dalam CyQL.
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

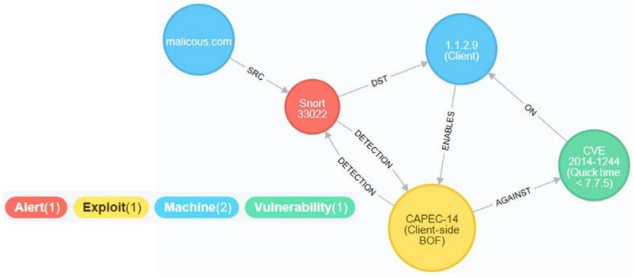
Ada beberapa fungsi bertipe *query*, seperti memetakan *network topology*, mengkorelasikan peringatan-peringatan, dan mengiterasi lintasan yang terdapat kerentanan. *Grammar* ini juga mengandung aturan untuk *parsing* entitas-entitas seperti alamat IP dan nama *host*.

Berikut adalah contoh graf pengetahuan yang siap digunakan untuk *query*. Pada graf tersebut, telah terdapat data mengenai pola serangan, mesin, *subnet* (subjaringan), *firewall*, dan kerentanan data. Lalu, ditambahkan topologi dari jaringan, yaitu sisi yang menunjukkan kebersisian dari *domain* dan *firewall* yang berhubungan. Selain itu, juga ditambahkan detil mengenai kerentanan data dan pola serangan.



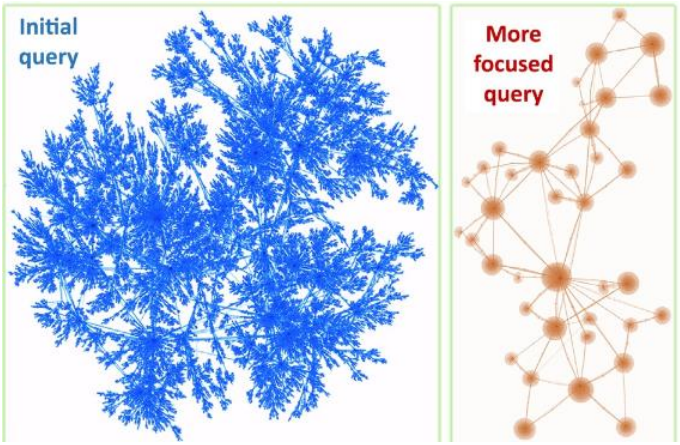
Gambar 14. Graf untuk *Query*
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

Berikut adalah graf *query* yang menunjukkan contoh peringatan akan terjadinya sebuah serangan. Graf ini menunjukkan bahwa korban dari serangan ini memang memiliki kerentanan yang berkaitan dengan suatu pola serangan tertentu dan dapat dideteksi oleh detector melalui analisis graf.



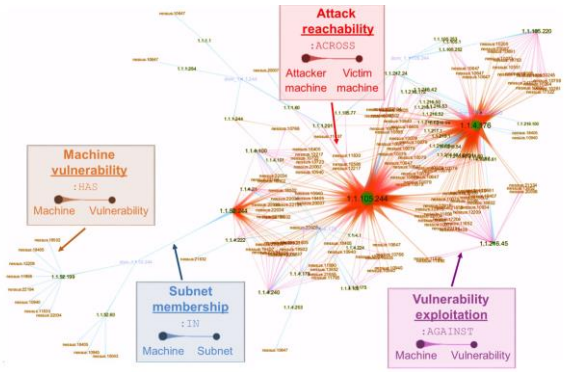
Gambar 15. Graf *Query*
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

Berikut adalah contoh graf hasil *query* dan subgrafnya untuk lebih fokus ke suatu bagian yang lebih spesifik.



Graf 16. *Dataset*
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

Dan berikut adalah contoh graf *query* yang lengkap, yang merupakan hasil transformasi dari graf serangan siber yang diolah oleh *tools*, seperti TVA (alat untuk pemodelan), menjadi graf yang telah mengandung komponen-komponen yang sesuai dengan graf pengetahuan atau basis data dari CyQL.



Gambar 17. Graf *Query* untuk Diproses
(Sumber : https://csis.gmu.edu/noel/pubs/2016_Cognitive_Computing_chapter.pdf)

V. KESIMPULAN

Graf memiliki berbagai aplikasi pada kehidupan sehari-hari. Salah satunya adalah dalam keamanan siber. Keamanan siber telah menjadi suatu hal yang penting karena maraknya serangan siber. Namun, alat yang ada untuk mengolah data dalam jumlah besar memiliki performa yang tidak terlalu baik. Oleh karena itu, pemanfaatan analisis dan visualisasi graf dapat sangat membantu dalam meningkatkan keamanan siber.

VI. UCAPAN TERIMA KASIH

Penulis mengucap syukur kepada Tuhan Yang Maha Esa karena atas berkat dan rahmatnya, Penulis dapat menyelesaikan karya tulis berjudul "Pemanfaatan Analisis dan Visualisasi Graf dalam Keamanan Siber". Penulis juga berterima kasih kepada keluarga Penulis yang telah memberi semangat untuk menyelesaikan karya tulis ini. Selain itu, Penulis juga berterima kasih kepada Bu Harlili, dosen pengampu Mata Kuliah Matematika Diskrit untuk Kelas 2, atas segala ilmu dan pedoman yang telah diberikan. Tak lupa, Penulis juga berterima kasih kepada teman-teman Penulis yang telah membantu dan memberikan semangat.

DAFTAR PUSTAKA

[1] Anonim. *Dasar-dasar Teori Graph*. staff.ayu_ws.gunadarma.ac.id. (diakses 1 Desember 2019, pukul 20.30 WIB).
[2] Anonim. *Bab II Landasan Teori*. https://dspace.uii.ac.id/bitstream/handle/123456789/12038/06.2%20bab%202.pdf?sequence=7&isAllowed=y. (diakses 2 Desember 2019, pukul 11.25 WIB).
[3] Cisco. *What is Cybersecurity?*. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works. (diakses 30 November 2019, pukul 18.00 WIB).
[4] Jean. *How Cisco Uses Graph Analytics to Identify Threats* https://linkurio.us/blog/cyber-security-how-cisco-use-graph-analytics-to-identify-threats/. (diakses 30 November 2019, pukul 21.15 WIB).
[5] Jean. *Cyber Security : How to Use Graphs to Do An Attack Analysis*. https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/. (diakses 3 Desember 2019, pukul 21.45 WIB).
[6] Lunkurious. *Graph Data Visualisation for Cyber-Security Threats Analysis*. https://linkurio.us/blog/graph-data-visualisation-cyber-security-threats-analysis/. (diakses 3 Desember 2019, pukul 23.18 WIB).
[7] Munir, Rinaldi. *Graf*. http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2015-2016/Graf%20(2015).pdf (diakses 1 Desember 2019, pukul 19.00 WIB).
[8] Noel, S.; Harley, E.; Tam, K.H.; Limiero, M.; and Share, M. *CyGraph : Graph-Based Analytics and Visualization for Cybersecurity*. (diakses 4 Desember 2019, pukul 00.35 WIB).
[9] Phintraco Group. *Pentingnya Cyber Security*. http://www.phintraco.com/pentingnya-cyber-security/. (diakses 2 Desember 2019, pukul 11.50 WIB).
[10] Sumba, Xavier. *A Gentle Introduction to Graph Theory*. https://towardsdatascience.com/graph-theory-132122ac38f2. (diakses 1 Desember 2019, pukul 17.48 WIB).
[11] Taylor, Hugh. *What are Cyber Threats: How They Affect You and What to Do About Them*. https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/. (diakses 30 November 2019, pukul 15.30 WIB).

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 4 Desember 2019

Florencia Wijaya 13518020