METRIK KEAMANAN BERBASIS GRAF UNTUK MENINGKATKAN KEAMANAN PADA MOBILE e-VOTING: SEBUAH SURVEY

Teguh Nurhadi Suharsono
Teknik Informatika Universitas Sangga Buana YPKP
Jl. PHH Mustofa (Suci) No.68 Bandung, Indonesia
E-mail : teguhns21@gmail.com

Abstract

Grup metrik keamanan berbasis graf dapat digunakan untuk mengevaluasi keamanan jaringan dari suatu jaringan komputer. Peningkatan jumlah host dan vulnerabilitas pada jaringan menyebabkan penurunan keamanan jaringan. Sistem e-Voting membutuhkan perhatian yang tinggi terhadap persyaratan keamanan. Pada penelitian ini dikembangkan ke arah mobile e-voting.

Keywords— metrik keamanan jaringan; graf; mobile e-voting;

I. PENDAHULUAN

Pada jaringan komputer terdapat vulnerabilitas yang ada pada host di jaringan. Vulnerabilitas ini memungkinkan penyusup untuk masuk ke dalam jaringan komputer. Urutan vulnerabilitas yang dilalui oleh penyusup dapat digambarkan menjadi suatu graf serangan. Graf serangan merupakan sebuah abstraksi yang menggambarkan cara penyerang melanggar kebijakan keamanan dengan cara memanfaatkan saling ketergantungan di antara berbagai vulnerabilitas yang ada. Metrik keamanan jaringan yang diukur dari graf serangan disebut metrik keamanan berbasis graf serangan[1]. Sistem mobile e-Voting membutuhkan perhatian yang tinggi terhadap persyaratan keamanan. Oleh sebab itu dibutuhkan metrik keamanan berbasis graf serangan untuk meningkatkan keamanan pada sistem mobile e-voting.

II. KEAMANAN

Keamanan adalah suatu proses menyediakan confidentiality (kerahasiaan), integritas dan availability (ketersediaan) terhadap suatu entitas berdasarkan suatu policy (kebijakan) [2].

Keamanan berkaitan erat dengan threat (ancaman) dan vulnerabilitas. Pengertian threat dan vulnerabilitas [3] adalah sebagai berikut:

Ancaman adalah suatu kondisi lingkungan yang mempunyai potensi menyebabkan kehilangan atau kemacetan.

Jenis threat dapat dibedakan menjadi:

1. Ancaman fisik (misalnya kebakaran, banjir, kegagalan bangunan atau kegagalan daya).
2. Ancaman peralatan (misalnya CPU, jaringan, atau kegagalan media penyimpanan).
3. Ancaman manusia (misalnya kesalahan operator atau desain, pencurian sumber daya).

Vulnerabilitas adalah pengaruh kemungkinan suatu ancaman menjadi kenyataan dan berhubungan dengan kelemahan pada sistem yang mungkin tereksploitasi dan menyebabkan kehilangan atau kemacetan.

III. KONSEP *MOBILE E-VOTING*

Adapun konsep mobile e-voting yang akan dibahas adalah:

1. Mobilitas berkaitan dengan tempat yang bisa dimana saja.
2. Registrasi dilakukan langsung dengan sistem aplikasi.
3. Seluruh data divalidasi melalui sistem aplikasi.
4. Proses otentifikasi berhadapan langsung dengan sistem aplikasi.
5. Tidak membutuhkan Tempat Pemungutan Suara (TPS) di suatu tempat, jadi pemilih bisa melakukan pemilihan di mana saja.
6. Rekapitulasi hasil perhitungan suara dilakukan secara otomatis.

IV. PERSYARATAN KEAMANAN MOBILE E-VOTING

Persyaratan keamanan *mobile e-voting* dibagi menjadi: persyaratan umum, persyaratan khusus, dan persyaratan tambahan. Daftar persyaratan berdasarkan Fujioka dkk. [4],Cranor dan Cytron [5], Salini dan Kanmani [6] , Wu dkk. [7], dan Adeshina dan Ojo [8], sebagai berikut:

A. Persyaratan Umum

Berupa persyaratan yang berlaku untuk semua sistem berbasis teknologi informasi dan komunikasi, yakni:

a. Kerahasiaan (confidentiality).

Semua data yang disimpan, diolah, dan dipertukarkan melalui jaringan komunikasi harus dijamin agar hanya bisa diakses oleh pihak yang berhak, misalnya: detil informasi tentang data diri pemilih harus dijamin tidak terbuka untuk publik.

b. Integritas (integrity).

Semua data harus dijamin tidak mengalami perubahan yang tidak sah, misal: basis data yang berisi hasil pemungutan suara harus dijaga agar tidak termodifikasi oleh siapapun secara tidak sah.

c. Autentikasi (authentication).

Sistem harus bisa dan memberikan fasilitas kepada semua pihak terkait untuk membuktikan kebenaran klaim identitasnya, misal: semua pihak (pemilih, kandidat, petugas pemilihan, saksi dll.) harus terlebih dahulu dapat menunjukkan bukti identitasnya sebelum berinteraksi dengan sistem.

d. Ketersediaan (availability).

Sistem harus dijamin dalam kondisi yang baik dan menyediakan layanan sebagaimana dijanjikan dengan derajat ketersediaan tertentu, misal: harus diupayakan dan dijamin bahwa sistem e-voting akan tersedia dan dapat diakses dalam 99,9999% dari seluruh waktu pemilihan yang telah ditetapkan.

B. Persyaratan Khusus

Berupa persyaratan yang secara khusus muncul dalam konteks e-voting, yaitu:

a. Eligibility: hanya orang yang ada dalam daftar pemilih sah yang dapat mengikuti pemungutan suara dan setiap pemilih yang sah hanya boleh sekali menggunakan hak pilihnya (memasukkan suara).

b. Anonymity: tidak ada siapapun (atau apapun) yang dapat merunut hubungan antara pilihan (suara) dengan pemilih yang memasukkannya.

c. Privacy: tidak ada pemilih yang memiliki cukup bukti tentang isi pilihannya dan dapat menunjukkannya kepada pihak lain.

d. Accuracy: tidak ada siapapun (atau apapun) yang dapat mengubah, menghapus, atau menduplikasi suara yang sah.

e. Verifiability: setiap pemilih harus dapat memeriksa apakah pilihannya telah tercatat dengan benar dan sistem dapat menunjukkan bahwa semua suara sah telah dihitung dengan benar.

f. Fairness: semua suara (pilihan) yang telah masuk ke sistem dan jumlah perolehan suara sementara tiap kandidat tidak dapat diketahui oleh siapapun sebelum pengumuman hasil akhir resminya.

g. Dispute-freeness: sistem harus menyediakan mekanisme dan artefak yang dibutuhkan untuk menyelesaikan sengketa yang mungkin muncul di semua tahapan.

h. Auditability: sistem harus dapat diaudit untuk menjamin semua prosesnya sesuai dengan spesifikasi dan semua ketidaksesuaian dapat ditangani dengan benar.

C. Persyaratan Tambahan

Meskipun bukan merupakan persyaratan yang secara langsung terkait dengan keamanan, namun hal-hal di bawah ini akan dapat membantu kemudahan pengelolaan, menaikkan tingkat keikutsertaan dalam pemungutan suara, dan sedikit banyak akan mempengaruhi upaya penjaminan keamanan sistem e-voting secara keseluruhan:

a. Kenyamanan (convenience).

Pemilih akan merasa nyaman jika dapat memasukkan pilihan atau suaranya melalui satu sesi pemungutan suara dengan cepat dan mudah, tanpa membutuhkan perangkat dan ketrampilan khusus.

b. Efisiensi (efficiency).

Penyelenggara pemungutan suara akan terbantu jika sistem e-voting dirancang untuk beroperasi dengan kebutuhan sumber daya komputasi dan waktu proses seminimal mungkin.

c. Fleksibilitas (flexibility).

Dengan adanya bermacam kebutuhan untuk meminta pendapat, sistem e-voting perlu dirancang untuk dapat menerima bermacam format kartu suara (misal: pilihan tunggal, pilihan jamak, pemberian nilai untuk tiap kandidat, penetapan urutan kandidat, penulisan jawaban terbuka dll.).

d. Mobilitas (mobility). Partisipasi pemilih diharapkan akan meningkat jika sistem e-voting memberikan keleluasaan kepada pemilih untuk dapat memasukkan suaranya di berbagai lokasi atau melalui beragam media yang tersedia dan dapat diakses dengan mudah oleh pemilih.

Properti ini adalah salah satu faktor yang memberikan kontribusi besar dalam memperumit masalah keamanan pada sistem e-voting.

V. METRIK DAN *MEASUREMENT*

Definisi metrik menurut [9] adalah nilai yang memfasilitasi pengambilan keputusan dan diturunkan dari pengukuran.

Menurut [2] metrik adalah hasil sedangkan measurement adalah aktivitas. Pengukuran adalah aktivitas suatu pelaksanaan observasi dan pengumpulan data dalam usaha untuk memperoleh pandangan praktis terhadap apa yang sedang dicoba untuk dipahami. Pengumpulan data keamanan sangatlah penting untuk melaksanakan program keamanan yang efektif. Namun jika tanpa konteks untuk data tersebut dan ide tentang alasan mengapa data itu dikumpulkan dan untuk tujuan apa data itu dikumpulkan, maka keterbatasan dalam menggambarkan pengukuran tersebut akan terbatas hanya pada istilah terabytes dari data log dan volume rak yang ditempati oleh laporan auditor.

Dalam [10] [11], metrik adalah standar yang konsisten untuk suatu pengukuran.Metrik yang baik seharusnya dapat diukur secara konsisten, murah memperolehnya, dinyatakan dalam bilangan kardinal atau persentase, dinyatakan oleh sedikitnya satu satuan pengukuran, spesifik kontekstual (cukup relevan dengan pengambil keputusan sehingga dapat diambil suatu keputusan).

VI. METRIK KEAMANAN

Idika dalam [9] menyatakan bahwa metrik keamanan adalah nilai-nilai yang dihasilkan dari pengukuran suatu atribut entitas (yang telah diidentifikasi) yang mempengaruhi keamanan fisik, personil, Teknologi Informasi (TI) atau operasional.

Krautsevich [12] menyatakan bahwa metrik keamanan adalah tools untuk menyediakan informasi yang benar dan terkini tentang keadaan (state) dari keamanan. Informasi ini sangat penting untuk mengelola keamanan secara efisien.

Metrik keamanan dapat diklasifikasikan menjadi beberapa kategori yaitu [13]:

a. Return on investment (ROI) metric.

b. Resiliency metric.

c. Compliance metric.

ROI metric mengukur keuntungan moneter suatu organisasi melalui sumber daya yang didedikasikan terhadap kendali keamanan.

Resiliency metric mengukur kemampuan suatu organisasi untuk memelihara layanan yang dapat diterima dengan kehadiran suatu serangan atau kegagalan.

Compliance metric mengukur seberapa baiknya suatu organisasi dalam mematuhi aturan atau standar.

VII. METRIK KEAMANAN JARINGAN

Metrik keamanan jaringan adalah nilai-nilai yang dihasilkan dari pengukuran suatu atribut entitas (yang dapat diidentifikasi) pada suatu jaringan yang mempengaruhi keamananfisik, personil, IT atau operasional [9].

Metrik keamanan jaringan dapat dibagi menjadi dua kategori [9] yaitu kelas primer dan kelas sekunder.

Kelas primer dari metrik keamanan jaringan adalah architectural-based metric dan performance-based metric.

Kelas sekunder dari metrik keamanan jaringan yaitu time-based metric, probability-based metric dan complexity-based metric.

Architectural-based metric mengukur atribut internal dari suatu jaringan. Atribut internal jaringan misalnya layanan yang tersedia pada jaringan, konektivitas dari host-host pada jaringan, dan vulnerabilitas. Metrik keamanan berbasis graf serangan termasuk ke dalam kategori architectural-based metrics.

Performance-based network security metrics mengukur atribut eksternal jaringan.Atribut eksternal jaringan misalnya kinerja manusia (human performance).

Probability-based network security metrics menggunakan probabilitas untuk memperoleh hasil yang diinginkan. Probabilitas dapat menyatakan suatu kemungkinan jaringan diserang, penyerang memilih suatu aksi, penyerang berhasil menembus kebijakan keamanan, atau penyerang mengeksploitasi vulnerabilitas tertentu. Probabilitas tersebut boleh memasukkan faktor sulitnya mengeksploitasi suatu vulnerabilitas. Kemungkinan ini menyebabkan mengapa perlu dibahas probabilitas dan kompleksitas secara bersamaan.

Time-based network security metrics menghasilkan suatu nilai waktu sebagai hasil.Time-based network security metrics digunakan untuk mengukur seberapa cepat suatu jaringan atau organisasi dapat ditembus atau seberapa cepat jaringan atau organisasi dapat merespon suatu serangan.

VIII. GRAF

Graf [1] adalah struktur diskrit yang berisi titik-titik dan sisi-sisi dimana sisi-sisi tersebut menghubungkan titik-titik yang bersesuaian. Jadi, sebuah graf dinyatakan oleh dua himpunan yaitu himpunan titik (V) dan himpunan sisi (E).

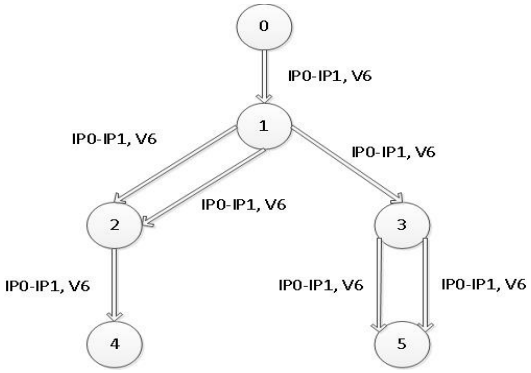
Sebuah graf G=(V,E) yang terdiri dari V, himpunan tak kosong berisi titik-titik (nodes) dan E, himpunan yang berisi sisi-sisi (edges). Setiap sisi memiliki satu atau dua titik yang berasosiasi dengan sisi tersebut yang disebut titik akhir (endpoints).Sebuah sisi menghubungkan titik-titik akhirnya.

Graf yang berisi infinite vertices V disebut infinite graph sedangkan graf yang berisi finite vertices V disebut finite graph. Pada penelitian ini digunakan finite graph.

Pada penelitian ini digunakan tiga jenis graf yang ditinjau dari arti titik dan garis pada graf. Adapun ketiga jenis graf yang digunakan yaitu:

1. Graf Status

Pada graf status, setiap titik pada graf menyatakan status jaringan pada saat tertentu. Setiap sisi pada graf menyatakan IP awal dan IP akhir yang dilalui oleh attacker.

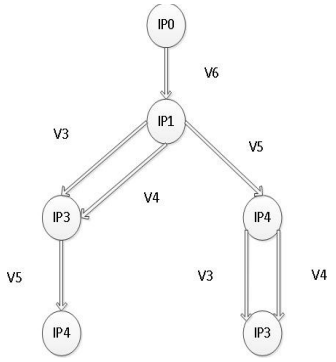


Gambar 1. Contoh Graf Status [1]

Pada Gambar 1. diperlihatkan contoh Graf Status.

2. Graf Akses Host (Graf Host)

Pada graf akses host, setiap titik pada graf menyatakan host. Setiap sisi pada graf akses host menyatakan vulnerabilitas yang dieksploitasi.

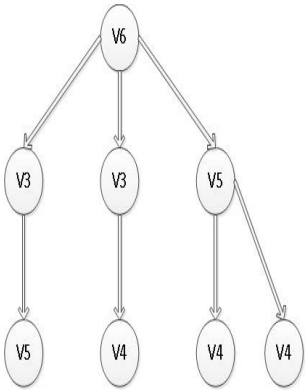


Gambar 2. Contoh Graf Host [1]

Pada Gambar 2. diperlihatkan contoh Graf Host.

3. Graf Vulnerabilitas

Pada graf vulnerabilitas, setiap titik pada graf menyatakan vulnerabiltas yang dieksploitasi. Setiap sisi pada graf menyatakan host awal dan host akhir dari setiap eksploitasi terhadap vulnerabilitas.



Gambar 3. Contoh Graf Vulnerabilitas [1]

Pada Gambar 3. diperlihatkan contoh Graf Vulnerabilitas.

IX. PENELITIAN SEBELUMNYA

Penelitian Metrik Keamanan Berbasis Graf Serangan sebelumnya dapat dilihat pada Tabel 1. Network Compromise Percentage (NCP) didefinisikan sebagai prosentase host pada jaringan yang dapat diakses oleh penyerang menggunakan akses level user atau administrator [14].

Expected Risk (ER) untuk suatu layanan didefinisikan sebagai hasil kali dari peluang terjadinya sedikitnya satu dari vulnerabilitas baru akan mempengaruhi layanan pada periode waktu berikutnya dan nilai harapan dari keriskanan (severity) vulnerabilitas [15].

Security Risk (SR) didefinisikan sebagai metrik yang diukur berdasarkan faktor-faktor banyaknya lintasan serangan, jarak lintasan serangan dan banyaknya jenis exploit dalam lintasan serangan [16].

Exploited Vulnerability Percentage (EVP) didefinisikan sebagai prosentase vulnerabilitas yang tereksploitasi pada jaringan.Vulnerable Host Percentage (VHP) didefinisikan sebagai prosentase vulnerable host pada jaringan [17].

Pada disertasi [9] dibahas grup Metrik Keamanan Berbasis Graf Serangan digunakan untuk mengevaluasi keamanan suatu jaringan dan melakukan peningkatan keamanan jaringan. Tabel 2 berisi klasifikasi dari Metric Keamanan Berbasis Graf Serangan yang diajukan dalam disertasi [9].

Pada disertasi [1] dibahas tentang SWSP, SHP, SVP, EVP, VHP dengan Algoritma Graf Status Keamanan.

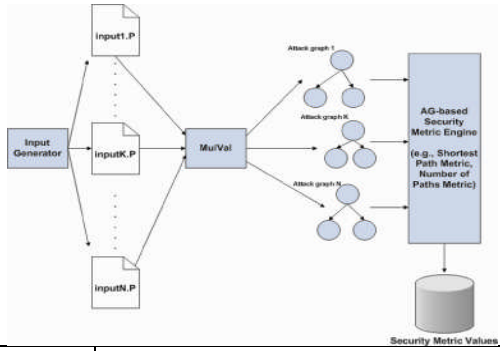
Tabel 1. Penelitian Metrik Keamanan Berbasis Graf Serangan

No.	Peneliti/ Tahun Penelitian	Metrik yang diajukan	Metode Network Hardening	Algoritma	Kompleksitas Waktu
1.	(Lippmann, R., Ingols, K., Scott, C., Piwowarski, Kratkiewicz, K., Artz, M., Cunningham, R., October 2006) [*14*]	Network Compromise Percentage (NCP)	-	-	-
2.	(Wang, L. Singhal, A. Jajodia, S., August 2007) [*18*]	Attack Resistance (AR)	-	breadth-first	$O(\|E\|^2)$

3.	(Wang, L. Islam, T. Long, T. Singhal, A. Jajodia, S., 2008) [*19*]	Attack Graph-based Probabilistic (AGP)	-	modified breadth-first search (BFS)	-
4.	(Ahmed, M. S., Al-Shaer, E., Khan, E., 2008) [*15*]	Expected Risk (ER)	Network risk measurement framework	-	-
5.	(Ingols, K., Chu, M. Lippmann, R., Webster, S., Boyer, S., 2009) [*20*]	-	NetSPA	Reachability	-
6.	(N. Idika, B. Marshall, and B. Bhargava., Apr. 2009.) [*21*]	KCA	Program Dinamis	Depth-first search	$O(nH^2B)$ $O(nHKB)$
	(Chen, F., Liu, A., Zhang, Y., Su, J., 2010) [*16*]	Security Risk	Weighted Greedy	Recursive, weighted-greedy	Recursive: $O(M^{n-1})$
8.	(Idika, 2010) [*9*]	SP, NP, NMPL, SDPL, MoPL, MePL, KCA	Program Dinamis	Depth-first search	$O(nH^2B)$ $O(nHKB)$
9.	(Viduto, 2012) [*22*]	-	Multiobjective Optimisation		
10.	(Purboyo, 2015) [*1*]	SWSP, SHP, SVP, EVP, VHP	User Based Network Hardening	Algoritma Graf Status Keamanan	$O(H^2)$

Tabel 2. Contoh Grup Metrik Keamanan Berbasis Graf Serangan [9]

Type	*Metric*
Decision	*SP Shortest Path* *NP Number of Paths* *NMPL Normalized Mean of Path Lengths* *NCP Network Compromise Percentage* *WA Weakest Adversary* *KCA K-step condition Accumulation*
Assistive	*MPL Mean of Path Lengths* *SDPL Standard Deviation of Path Lengths* *MoPL Mode of Path Lengths* *MePL Median of Path Lengths*



Gambar 1. Kerangka Kerja Percobaan [9]

Pada Gambar 1 dapat dilihat kerangka kerja percobaan (experiment framework) yang dilakukan pada penelitian disertasi Idika [9]. Pembangkit masukan (Input Generator) menghasilkan file masukan untuk Mulval. Tiap masukan yang dihasilkan yaitu input1.P, input2.P, input3.P,...,inputK.P, input(K+1).P, input(K+2).P, ..., input(N-1).P, inputN.P masing-masing dimasukkan ke MulVal untuk dibuatkan graf serangan yang bersesuaian. Pembangkit masukan ini melakukan generate vulnerabilitas pada tiap host di jaringan. Setiap graf serangan diukur menggunakan metrik keamanan jaringan berbasis graf. Metrik keamanan berbasis graf ini dihitung oleh AG-based Security Metric Engine. Untuk setiap graf serangan, nilai metrik keamanan berbasis graf disimpan dalam database.

Dalam [14] dijelaskan bahwa pertahanan secara mendalam (Defense in depth) merupakan strategi umum yang menggunakan beberapa lapis pertahanan untuk melindungi subnet kendali pengawasan dan akuisisi data (Supervisory Control and Data Acquisition-SCADA) dan sumber daya penting lainnya pada jaringan enterprise. Tools yang disebut Network Security Planning Architecture (NetSPA) juga dibahas. Tools ini dapat menganalisa aturan firewall dan vulnerabilitas yang digunakan untuk mengkonstruksi graf serangan. Graf serangan ini dapat menunjukkan bagaimana attacker dapat mengeksploitasi vulnerable host yang terlihat dengan tujuan mencapai target. NetSPA menghasilkan graf serangan dan secara otomatis menganalisanya untuk menghasilkan sekumpulan prioritas rekomendasi untuk mengembalikan pertahanan secara mendalam. Percobaan pada jaringan dengan jumlah host 3400 menunjukkan bahwa firewall seringkali tidak menyediakan pertahanan secara mendalam yang disebabkan oleh kesalahan konfigurasi dan vulnerabilitas yang tidak dihilangkan pada host. Pada semua kasus, sejumlah kecil rekomendasi disajikan untuk mengembalikan pertahanan secara mendalam. Simulasi pada jaringan yang memiliki 50.000 host menunjukkan bahwa pendekatan ini terskalakan

dengan baik untuk jaringan-jaringan sebesar jaringan enterprise.

Dalam [16], Chen dkk.menjelaskan bahwa graf serangan yang kompak secara implisit menunjukkan ancaman (*threat*) dari *multi-step attack* dengan mencoba urutan yang mungkin dari eksploitasi yang menyebabkan terkomprominya sumber daya yang penting pada jaringan enterprise dengan ribuan host. Pada makalah ini didiskusikan bagaimana menganalisa graf serangan yang kompleks untuk mempertahankan keamanan jaringan. Pengukuran risiko keamanan dari sumber daya kritis dijelaskan pada makalah ini. Solusi untuk menghilangkan vulnerabilitas agar sumber daya kritis tidak bisa dikompromisasi dengan biaya minimal juga dibahas. Pendekatan terskala dibuktikan mempunyai kompleksitas waktu polinomial dan dapat digunakan pada graf serangan yang memiliki ribuan host pada jaringan enterprise.

Dalam [20], Ingols dkk.menjelaskan bahwa dengan pengukuran secara akurat pada jaringan enterprise, graf serangan memungkinkan defender jaringan untuk memahami ancaman kritis dan memilih *countermeasure* yang paling efektif. Makalah ini menjelaskan peningkatan terhadap sistem graf serangan NetSPA yang diperlukan untuk memodelkan ancaman terkini (eksploitasi zero day dan client-side attack) dan countermeasure (sistem pencegahan intrusi, firewall proxy, firewall personal, dan host-based vulnerability scan).Analisis terhadap jaringan dengan 85 host menunjukkan bahwa client-side attack menemui ancaman serius. Waktu yang dibutuhkan untuk menganalisis jaringan dengan 40.000 host yang dilindungi oleh firewall personal adalah kurang dari dua menit.

Pada [23], Patel menjelaskan bahwa keamanan jaringan dan informasi sangat krusial dalam menjaga infrastruktur informasi yang besar agar tetap aman. Graf serangan merupakan tool untuk memodelkan keamanan jaringan yang meninjau vulnerabilitas individu pada sudut pandang global dimana host individu saling terhubung. Analisis terhadap informasi peringatan intrusi sangat penting untuk mengevaluasi sistem. Karena sebagian besar peringatan muncul dari intrusion detection system (IDS), maka menjadi sulit bagi ahli keamanan untuk menganalisis peringatan individu (individual alerts). Para peneliti menangani masalah ini dengan membuat cluster untuk peringatan individu seperti alamat IP sumber, alamat IP tujuan, nomorport dan lainnya. Pada makalah ini diajukan metode yang berbeda untuk pengklasteran. Barisan peringatan intrusi disiapkan dengan membagi peringatan berdasarkan pada interval waktu tertentu. Barisan peringatan intrusi ditinjau sebagai graf serangan sementara. Barisan diklasterkan mengggunakan teknik pengklasteran graf yang meninjau kemiripan dalam barisan sebagai faktor untuk menentukan kedekatan barisan. Pendekatan yang disarankan mengkombinasikan konsep graf serangan dan clustering pada barisan peringatan menggunakan teknik pengklasteran graf.

Dalam [24], Homer dkk.menjelaskan bahwa berbagai tool yang ada untuk menganalisis sistem jaringan perusahaan dan untuk menghasilkan graf serangan yang menggambarkan bagaimana penyerang dapat menembus ke dalam sistem. Makalah ini menyajikan metodologi yang dapat 1) secara otomatis mengidentifikasi bagian dari graf serangan yang tidak membantu pengguna untuk memahami masalah utama keamanan, dan 2) secara otomatis mengelompokkan langkah serangan yang serupa sebagai titik virtual pada model jaringan, untuk segera memudahkan pemahaman terhadap data. Kedua metode tersebut sangat penting untuk mengembangkan visualisasi graf serangan agar lebih berguna dalam manajemen konfigurasi untuk jaringan perusahaan yang besar.

Dalam [15], Ahmed dkk. menjelaskan bahwa evaluasi terhadap keamanan jaringan merupakan langkah esensial dalam mengamankan jaringan. Evaluasi ini dapat membantu profesional keamanan dalam menentukan keputusan yang optimal tentang bagaimana mendesain *countermeasure*, memilih arsitektur keamanan alternatif, dan secara sistematis mengubah konfigurasi keamanan agar keamanan meningkat. Bagaimana pun, keamanan jaringan tergantung pada sejumlah faktor yang berubah secara dinamis seperti penemuan vulnerabilitas dan ancaman baru, struktur kebijakan dan lalu lintas jaringan. Identifikasi, kuantifikasi dan validasi faktor-faktor tersebut menggunakan metrik keamanan adalah tantangan utama dalam bidang tersebut. Dalam makalah ini diajukan kerangka kerja metrik keamananyang mengidentifikasi dan mengkuantifikasi faktor risiko keamanan yang paling signifikan secara obyektif. Faktor-faktor ini mencakup vulnerabilitas yang ada, kecenderungan historis vulnerabilitas dari layanan yang bisa diakses secara remote, prediksi vulnerabilitas potensial untuk layanan jaringan umum, hingga ketahanan kebijakan terhadap rambatan serangan pada jaringan. Selanjutnya dibahas percobaan validasi secara menyeluruh menggunakan data vulnerabilitas dari National Vulnerability Database (NVD) untuk menunjukkan akurasi yang baik dari metrik yang diajukan. Beberapa penelitian terdahulu meninjau vulnerabilitas menggunakan analisis kode. Bagaimana pun, penelitian ini adalah yang pertama kali menggunakan informasi vulnerabilitas dan konfigurasi kebijakan keamanan publik.

X. KESIMPULAN

Berdasarkan dari uraian sebelumnya, maka dapat dilihat beberapa peluang untuk melakukan penelitian selanjutnya:

1. Mengembangkan metrik keamanan berbasis graf serangan pada *mobile e-voting* untuk meningkatkan keamanan.
2. Mengembangkan framework untuk mengevaluasi keamanan pada sistem *mobile e-voting*.
3. Dikembangkannya suatu algoritma untuk menghasilkan graf status keamanan jaringan yang akan dikonstruksi sehingga dapat dihitung metrik-metrik keamanan jaringan berbasis graf pada sistem *mobile e-voting*.

4. Melakukan pemilihan untuk konfigurasi *countermeasure* sehingga dapat menghitung risiko dan biaya total penerapan konfigurasi *countermeasure* pada sistem *moble e-voting.*

DAFTAR PUSTAKA

[1] T.W. Purboyo, B. Rahardjo , Kuspriyanto , and M.I. Detiena , "Pengembangan Metrik Keamanan Berbasis Graf," 2015.

[2] L Hayden, *IT Security Metrics. New York: The McGraw-Hill Companies*., 2010.

[3] S.M. Furnell, S. Katsikas , J. Lopez , and A. Patel , "Securing Information and Communications Systems: Principles, Technologies, and Applications," *Artech House, Inc.*, 2008.

[4] A. Fujioka, T. Okamoto , and K. Ohta , "A Practical Secret Voting Scheme," *Advances in Cryptology - AUSCRYPT '92*, 1992.

[5] L. F. Cranor and R. K. Cytron , "Sensus: A Security-Conscious Electronic," *Proceedings of the Hawai`i International Conference on System Sciences*, 1997.

[6] P. Salini and S. Kanmani , "Application of Model Oriented Security Requirements Engineering Framework for secure E-Voting," in *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, 2012, pp. 1–6.

[7] Z.-Y. Wu, J.-C. Wu, , S.-C. Lin , and C. Wang , "An electronic voting mechanism for fighting bribery and coercion," *J. Netw. Comput. Appl*, vol. 40, pp. 139–150, April 2014.

[8] S. A. Adeshina and A. Ojo , "Design imperatives for e-voting as a sociotechnical system," in *2014 11th International Conference on Electronics, Computer and Computation (ICECCO)*, 2014, pp. 1–4.

[9] Nwokedi C. Idika, *Characterizing and Aggregating Attack Graph-Based Security Metrics.*. PhD Dissertation. Purdue University. West Lafayette. Indiana, 2010.

[10] A. Jaquith, *Security metrics : replacing fear, uncertainty, and doubt*.: Pearson Education, Inc., 2007.

[11] T.W. Purboyo, B. Rahardjo , and Kuspriyanto , "Security Metrics: A Brief Survey," in *International Conference ICICI-BME*, 2011, pp. 8-9.

[12] L., Martinelli, F., Yautsiukhin, A. Krautsevich, "Formal approach to security metrics: What does "more secure" mean for you?," in *IEEE Paper IEEE/ASME International Conference on Mechatronic and Embedded Systems and Application*, 2010.

[13] D. Herrmann, *A Practical Guide to Security Engineering and Information Assurance*.: Auerbach Publications, 2002.

[14] Lippmann, R., Ingols, K., Scott, C., Piwowarski, Kratkiewicz, K., Artz, M., Cunningham, R., "Validating and restoring defense in depth using attack graphs," in *Military Communications Conference*, October 2006.

[15] Ahmed, M. S., Al-Shaer, E., Khan, E., "A novel quantitative approach for measuring network security.," in *Proceedings of IEEE INFO COM 2008.*, 2008.

[16] Chen, F., Liu, A., Zhang, Y., Su, J., "A Scalable Approach to Analyzing Network Security using Compact Attack Graph.," *JOURNAL OF NETWORKS, VOL. 5, NO. 5.*, 2010.

[17] T.W. Purboyo, B. Rahardjo, Kuspriyanto , and M.I. Detiena, "(2012): A New Metrics for Predicting Network Security Level," *Journal of Global Research in Computer Science (JGRCS)*, vol. Vol. 3 No. 3, pp. 68-72, 2012.

[18] Wang, L. Singhal, A. Jajodia, S., "Measuring overall security of network con-figurations using attack graphs," *Data and Applications Security XXI*, vol. vol. 4602, pp. 98–112, August 2007.

[19] Wang, L. Islam, T. Long, T. Singhal, A. Jajodia, S., *An attack graph-based probabilistic security metric*.: DAS 2008, LNCS 5094, pp. 283–296, 2008.

[20] Ingols, K., Chu, M. Lippmann, R., Webster, S., Boyer, S., "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs.," *Annual Computer Security Applications Conference (ACSAC) 25th*, 2009.

[21] N. Idika, B. Marshall, and B. Bhargava., "Maximizing Security given a Limited Budget," *Proc. TAPIA '09: Richard Tapia Celebration of Diversity in Computing*, Apr. 2009.

[22] Valentina Viduto, *A Risk Assessment and Optimisation Model for Minimising Network Security Risk and Cost*. Bedfordshire: University of Bedfordshire, 2012.

[23] H. Patel, *Intrusion Alerts Analysis Using Attack Graphs and Clustering*.: San Jose State University, 2009.

[24] J. Homer, A. Varikuti, X. Ou, and M.A. McQueen, *Improving Attack Graph Visualization Through Data Reduction and Attack Grouping.: Workshop on Visualization for Computer Security (VizSEC)*., 2008.