Jurnal Pendidikan dan Aplikasi Industri (UNISTEK)
Vol. 7 No.2 Agustus 2020
p-ISSN : 0126 – 4036
e-ISSN : 2716 - 0416

Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: *Systematic Review*

Agustani Bustami[1)] dan Syamsul Bahri[2)]

Program Studi Magister Ilmu Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta, Indonesia

[1)] abustami@gmail.com
[2)] syamsul8895@gmail.com

Abstrak. *Keamanan jaringan atau sistem informasi sangat berdampak dengan kehadiran berbagai ancaman atau serangan yang dapat menyebabkan kebocoran informasi sensitif dan rahasia serta penurunan kinerja organisasi. Terdapat beraneka ragam ancaman atau serangan pada keamanan jaringan atau sistem informasi seperti insider attacks, eavesdropping, poor configurations, lack of contingency, masquerading, man-in-the-middle-attack, virus attack atau denial of service attack dan lain sebagainya. Tanpa perlindungan yang memadai berupa keamanan jaringan atau sistem informasi, organisasi berisiko kehilangan aset informasi mereka. Teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari beragam ancaman atau serangan keamanan. Agar penentuan teknologi keamanan dapat sesuai dengan kebutuhan organisasi, maka diperlukan pemetaan terlebih dahulu antara jenis ancaman atau serangan dengan teknologi keamanan yang ada berdasarkan kepada aspek keamanan, yaitu: kerahasiaan (confidentiality), integritas (integrity) dan ketersediaan (availability). Firewall, IDS, antivirus system dan cryptographic system menjadi teknologi keamanan pilihan disebabkan kehandalan mereka dalam mengantisipasi dan melindungi jaringan atau sistem informasi pada aspek keamanan yang berbeda-beda.*

Kata kunci: *keamanan jaringan, serangan keamanan dan tindakan perlindungan, keamanan informasi, ancaman, serangan dan teknologi keamanan, tinjauan sistematis*

Abstract. *Network or information system security is highly impacted by the presence of various threats or attacks that can cause leakage of sensitive and confidential information and decrease organizational performance. There are various threats or attacks on network security or information systems such as insider attacks, eavesdropping, poor configurations, lack of contingency, masquerading, man-in-the-middle-attacks, virus attacks or denial of service attacks and so forth. Without adequate protection in the form of network or information system security, organizations having risk losing their information assets. Appropriate security technology can be established as an anticipation and protection from various threats or security attacks. In order to determine the security technology in accordance with the needs of the organization, it is necessary to first map the types of threats or attacks with the existing security technology based on security aspects, namely: confidentiality, integrity and availability. Firewalls, IDS, antivirus systems and cryptographic systems are the security technologies of choice due to their reliability in anticipating and protecting networks or information systems in different security aspects.*

Keywords: *network security, security attack and protective countermeasure*, *information security*, *threat, attack and security technology, systematic review*

I. Pendahuluan

Pesatnya perkembangan teknologi informasi saat ini menyebabkan meningkatnya pengiriman data dan informasi secara global. Selain tingginya manfaat yang dirasakan, tingkat risiko dan ancaman penyalahgunaan teknologi informasi juga semakin tinggi dan kompleks. Organisasi menjadi lebih rentan terhadap ancaman atau serangan jaringan atau keamanan informasi yang disebabkan oleh berbagai sumber baik dari aktivitas personil internal atau serangan peretas (Jouini, Rabai, & Aissa, 2014). Beraneka ragam ancaman atau serangan jaringan atau sistem informasi hadir berpotensi menggangu kinerja dan layanan organisasi seperti *insider attacks*, *poor configurations, lack of contingency, masquerading, man-in-the-middle-attack, virus attack* atau *denial of service attack* (Bhatia & Sehrawat, 2014)(Nurse et al., 2014)(Pawar & Anuradha, 2015)(Konakalla & Veeranki, 2013).

Tanpa perlindungan yang memadai berupa keamanan jaringan atau sistem informasi, organisasi berisiko kehilangan aset informasi mereka. Keamanan jaringan atau sistem informasi adalah proses dimana aset informasi dilindungi mencakup perlindungan atas kerahasiaan, integritas, dan ketersediaan aset informasi tersebut (Alabady, 2009). Keamanan jaringan atau sistem informasi terdiri dari seperangkat kebijakan dan pelaksanaan yang diterapkan untuk mencegah dan memantau akses tidak sah, modifikasi dalam sistem, penyalahgunaan, atau penolakan jaringan komputer dan sumber daya yang dapat diakses jaringan (Pawar & Anuradha, 2015)(Farooq, 2018).

Implementasi teknologi keamanan sebagai tindakan perlindungan menjadi pilihan dalam upaya melindungi aset informasi dari ancaman atau serangan jaringan atau sistem informasi. Berbagai teknologi keamanan hadir sebagai perlindungan keamanan atas ancaman atau serangan pada jaringan atau sistem informasi antara lain *firewall*, *cryptographic system*, IDS, SSL, *antivirus system, IPSec, authentication* dan lain sebagainya (Konakalla & Veeranki, 2013)(Gaigole & Prof, 2016)(Khan, 2017)(Sanghavi, Mehta, & Soni, 2010)(Farooq, 2018).

Permasalahan yang muncul dari studi yang penulis kumpulkan terkait dengan ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi yaitu terbatasnya studi yang melakukan pemetaan antara ancaman atau serangan jaringan atau sistem informasi yang ada dengan teknologi keamanan yang sesuai sebagai tindakan pengendaliannya.

Dengan demikian, penelitian ini bertujuan untuk melakukan *systematic review* atas studi-studi tentang ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi yang pernah dipublikasi, sehingga didapat pemetaan yang diharapkan berguna bagi penelitian selanjutnya. *Systematic review* ini tidak memberikan opini terhadap suatu analisis yang pernah dilakukan dari penelitian sebelumnya serta tidak menetapkan metode khusus dalam analisisnya.

RQ: Implementasi teknologi keamanan manakah yang sesuai dan dapat mengantisipasi jenis-jenis serangan jaringan atau sistem informasi?

Penyusunan penulisan dan penyajian hasil *systematic review* dibagi menjadi enam bagian pembahasan, yaitu Pendahuluan (Bagian 1), Bahan dan Metode (Bagian 2), Hasil dan Pembahasan (Bagian 3), serta diakhiri dengan Kesimpulan (Bagian 4).

II. Bahan Dan Metode

Systematic review ini disusun berdasarkan pedoman pelaporan PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-analyses*) (Liberati et al., 2009). Terdapat beberapa langkah dalam penelitian ini sesuai dengan pedoman tersebut, yaitu:

1) Mendefinisikan kriteria kelayakan;
2) Mendefinisikan sumber informasi;
3) Pemilihan studi;
4) Pengumpulan data; dan
5) Pemilihan item data.

Kriteria kelayakan

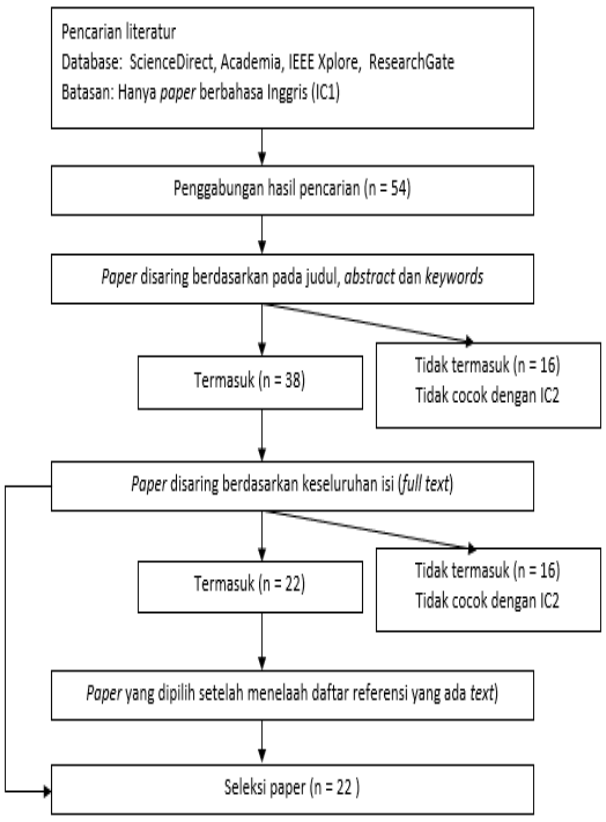
Inclusion criteria (IC) berikut ini ditetapkan sebagai pedoman *review*:

IC1: Penelitian asli dan *peer-reviewed* yang ditulis dalam Bahasa Inggris;

IC2: Penelitian yang bertujuan mengidentifikasi ancaman atau serangan dan implementasi teknologi keamanan sebagai tindakan perlindungan pada keamanan jaringan atau sistem informasi.

Hanya *paper* yang ditulis dalam bahasa Inggris (IC1) yang dipilih, dengan pertimbangan Bahasa Inggris adalah bahasa yang umum digunakan oleh para peneliti di komunitas ilmiah. IC2 dimasukkan guna menjawab pertanyaan penelitian (*research question*).

Ketertarikan penulis tidak terbatas hanya pada serangan dan teknologi keamanan sebagai perlindungan pada jaringan atau sistem informasi. Selain itu, penulis juga tertarik pada ancaman yang berpotensi menggangu kinerja dan layanan organisasi. Gambar 1 adalah diagram alir PRISMA yang menjelaskan langkah-langkah pekerjaan penulis dalam melakukan *systematic review*.



Gambar 1. Diagram Alir PRISMA

Sumber informasi

Paper-paper yang kami butuhkan dalam melakukan *systematic research* ini berasal dari database studi akademis, yaitu ScienceDirect, Academia, IEEE Xplore, dan ResearchGate. Penulis hanya mengakses *paper* yang dalam upaya mendapatkannya tidak ada persyaratan. Selain itu, penulis menelaah daftar referensi yang terdapat dalam *paper* untuk menemukan studi yang relevan.

Pemilihan studi

Pemilihan studi dilakukan dalam fase-fase berikut:

1) Pencarian kata kunci, dipilih sesuai dengan minat penelitian penulis dalam meninjau ancaman atau serangan keamanan jaringan atau sistem informasi dan teknologi keamanan yang sesuai sebagai tindakan perlindungannya. Kata kunci yang digunakan dalam pencarian paper pada database yang disebutkan di bagian II.B adalah "*network security*", "*security attack and protective countermeasure*", "*information security*", dan "*threat, attack and security technology;*"
2) Eksplorasi dan pemilihan judul, abstrak, dan kata kunci dari *paper* yang diidentifikasi dilakukan berdasarkan kriteria kelayakan;
3) Pembacaan lengkap atau sebagian *paper* yang memenuhi kriteria kelayakan dilakukan untuk menentukan apakah *paper* tersebut layak masuk dalam tinjauan;
4) Daftar referensi paper ditelaah untuk menemukan studi yang relevan.

Fase-fase tersebut di atas dilakukan secara kolaborasi oleh seluruh penulis yang melakukan *systematic review* ini. Sekiranya terdapat perbedaan, maka dilakukan pembahasan sampai dicapai kesepakatan bersama.

Pengumpulan data

Pengumpulan data dilakukan secara manual menggunakan instrumen tabel ekstrasi data yang terdiri dari: judul, penulis, tahun, nama jurnal/konferensi, tipe *paper*, topik, metode penelitian, hasil pembahasan dan kesimpulan. *Paper* yang relevan atau berpotensi relevan dinilai secara bersama-sama. Penilaian terdiri dari membaca teks lengkap dan data yang diekstrasi. Setiap perbedaan diselesaikan melalui diskusi antara penulis.

Pemilihan item data

Informasi yang diambil dari setiap *paper* terdiri dari: 1) penjelasan tentang keamanan jaringan atau sistem informasi; 2) ancaman atau serangan keamanan; 3) teknologi keamanan yang ada sebagai perlindungan.

III. Hasil Dan Pembahasan

Seleksi *paper*

Hasil pencarian dalam *database* yang dipilih memberikan total 54 paper yang ditulis dalam bahasa Inggris dari tahun 2009 hingga 2019, cocok dengan kata kunci yang perlu dianalisis. Selanjutnya, *paper-paper* tersebut disaring berdasarkan judul, abstrak, dan kata kunci. Tersisa 38 *paper* yang kemudian ditinjau berdasarkan teks lengkapnya, sebanyak 16 paper dibuang karena tidak memenuhi kriteria IC2. Akhirnya terpilih 22 *paper* yang memenuhi kriteria kelayakan dan menjadi bahan dalam *systematic review* ini.

Karakteristik *paper*

Informasi detil dari 22 *paper* yang terpilih dapat dilihat pada Tabel 1 tentang ekstrasi data final. Ekstrasi data final ini adalah tabel ekstrasi data yang hanya berisi *paper-paper* terpilih berdasarkan kriteria-kriteria yang ada pada proses seleksi paper (Bagian III.A).

Tabel 1. Ekstrasi Data Final

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
1	Singh et al., 2011	International Journal of Computer Trends and Technology	Review Paper	Ancaman, Serangan, Teknologi Keamanan	Kualitatif	Ancaman: External versus internal attacks, Passive versus active attacks, Mote-class versus laptop-class attacks. Serangan: Interuption, DoS, Sybil, Blackhole, Wormhole. Teknologi: SPIN, TinySec, LEAP	Keamanan di WSN telah menarik banyak perhatian dalam beberapa tahun terakhir. Fitur yang menonjol dari WSN membuatnya sangat menantang untuk merancang protokol keamanan yang kuat sambil tetap mempertahankan biaya overhead yang rendah

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
2	Stosic & Velickovic, 2013	Journal of Process Management – New Technologies	Review Paper	Serangan, Teknologi Keamanan	Kualitatif	Serangan: Cutting or breaking, Interception, Changed, Fabrication. Teknologi: Kriptografi, Otentikasi. Otorisasi	Ada banyak teknik yang membantu melindungi sistem jaringan: kriptografi, otentikasi, otorisasi
3	Jouini et al., 2014	Procedia Computer Science	Research Paper	Ancaman	Kuantitatif	Ancaman: External Threats, Internal Threats	Untuk meningkatkan pemahaman tentang ancaman keamanan, diusulkan model klasifikasi ancaman keamanan yang memungkinkan untuk mempelajari dampak kelas ancaman karena ancaman bervariasi dari waktu ke waktu
4	Konakalla & Veeranki, 2013	International Journal of Computer Science and Mobile Computing	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Virus, System and Boot Record Infectors, Eavesdropping, Hacking, Worms, Trojan, IP Spoofing, DoS. Teknologi: Cryptographic systems, Firewall, IDS, Anti-Malware Software, IPSec, SSL	Keamanan sangat penting dan harus dipastikan agar pengguna internet dapat memiliki kepercayaan diri terlibat dalam kegiatan di Internet.
5	Gaigole & Prof, 2016	International Journal of Computer Science and Mobile Computing	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Passive attacks, Active attacks, Distributed attacks. Teknologi: Cryptographic systems, Firewall, IDS, Anti-Malware Software, IPSec, SSL	Keamanan jaringan menjadi sangat penting karena kekayaan intelektual yang dapat dengan mudah diperoleh melalui internet. Ada berbagai jenis serangan yang dapat terjadi ketika dikirim melalui jaringan. Dengan mengetahui metode serangan, memungkinkan keamanan yang sesuai muncul. Banyak bisnis mengamankan diri mereka dari internet melalui firewall dan mekanisme enkripsi.

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
6	Khan, 2017	International Journal of Advanced Research in Computer Science	Review Paper	Ancaman, Serangan, Teknologi Keamanan	Kualitatif	Ancaman: Insider attacks, Threats Insider attacks Lack of contingency, Poor configuration. Serangan: Passive attacks, Active attacks, Phishing, Social Engineering, Hijack Teknologi: Firewall, Antivirus, IDS,	Terdapat berbagai jenis ancaman dan serangan pada sistem jaringan dan langkah-langkah antisipasi umum untuk mengurangi situasi merugikan.
7	Sanghavi et al., 2010	International Journal of Scientific and Research Publications	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Eavesdropping, Viruses, Worms, Trojans, Phishing, IP Spoofing, DoS. Teknologi: Cryptographic systems, Firewall, IDS, Antimalware, SSL,	Gabungan penggunaan firewall, deteksi intrusi, dan mekanisme otentikasi akan terbukti efektif dalam menjaga kekayaan intelektual dalam waktu dekat. Bidang keamanan jaringan mungkin harus berkembang lebih cepat untuk menghadapi ancaman lebih lanjut di masa depan
8	Farooq, 2018	International Journal of Advanced Research in Computer Science	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Active attacks, Passive attacks Teknologi: Firewall, Cryptography, SSL, IDS, Antivirus	Untuk menjaga privasi, keamanan dan untuk mencegah serangan cyber, banyak perusahaan dan pemerintah mengambil banyak langkah, tetapi keamanan cyber masih menjadi perhatian besar.
9	Kotkar et al., 2013	International Journal of Innovative Research in Computer and Communication Engineering	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: MAC Flooding, Hijacking, IP Spoofing, DoS Teknologi: IEEE 802.1X suites, Encryption, Authentication, Firewall, IDS	Ethical hacker dapat berbuat pada jaringan jika jaringan lemah
10	Geric & Zejko, 2007	International Journal of Scientific and Research Publications	Research Paper	Ancaman	Kuantitatif	Ancaman: Errors and omissions, Fraud and theft, Employee sabotage,	Klasifikasi yang ada sudah ketinggalan zaman, terutama dalam konteks kompatibilitas dan komparabilitasnya.

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						Hackers, Malware	Untuk mengatasi masalah ini model C3 yang diusulkan dapat digunakan. Karakteristik utamanya adalah modelnya fleksibel, dinamis, dan multidimensi yang memberinya keunggulan tertentu dibandingkan dengan model klasifikasi lain yang disebutkan.
11	Safianu et al., 2016	International Journal of Computer Applications	Research Paper	Ancaman, Serangan	Kuantitatif	Ancaman: External Threats, Internal Threats. Serangan: Social engineering, SQL injection, Cross Site Scripting (XSS), Brute force attack	Keamanan informasi tidak dapat digambarkan hanya sebagai masalah teknis. Komputer dioperasikan oleh orang dan ini berarti bahwa keamanan informasi juga merupakan masalah faktor manusia. Oleh karena itu disarankan, agar pelanggaran informasi dan data dapat diatasi, organisasi harus mengadopsi kerangka kerja keamanan holistik, dengan memasukkan faktor manusia
12	Conteh & Schmick, 2016	International Journal of Advanced Computer Research	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Social engineering Teknologi: IDS, IPS, Firewall	Teknologi memiliki peran untuk dimainkan dalam mengurangi dampak serangan rekayasa sosial, kerentanan berada pada perilaku manusia, impuls manusia dan kecenderungan psikologis yang dapat dipengaruhi melalui pelatihan
13	Bays et al., 2015	Journal ofInternet Services andApplications	Research Paper	Ancaman, Teknologi Keamanan	Kuantitatif	Ancaman: Information leakage, Identity fraud, Physical resources overloading. Teknologi: Access control, Authentication, Cryptography, Firewall	Hal ini diperlukan untuk memberikan perlindungan terhadap infrastruktur jaringan virtual untuk memungkinkan penggunaannya dalam lingkungan skala nyata.

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
14	Jain et al., 2012	International Journal Math and Computer Science	Review Paper	Serangan, Teknologi Keamanan	Kualitatif	Serangan: Active attacks, Passive attacks,. Teknologi: Firewall, Cryptography, SSL, IDS, Antivirus	Kecanggihan teknologi menambah kompleksitas dan kurva belajar yang lebih curam; dan kompleksitas menyebabkan pengawasan, sehingga menciptakan celah keamanan
15	Alabady, 2009	International Arab Journal of e-Technology	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Session replay attacks, Rerouting, Masquerade attacks, Hijacking, DDoS. Teknologi: Firewall, IDS	Firewall memberikan kontrol akses tambahan atas koneksi dan lalu lintas jaringan dan melakukan otentikasi pengguna. Menggunakan firewall dan router bersama-sama dapat menawarkan keamanan yang lebih baik daripada salah satu saja. Konfigurasi filter router yang buruk dapat mengurangi keamanan keseluruhan jaringan, mengekspos komponen jaringan internal untuk pemindaian dan serangan
16	Bhatia & Sehrawat, 2014	International Journal for Scientific Research & Development	Research Paper	Ancaman, Serangan, Teknologi Keamanan	Kuantitatif	Ancaman: Insider attacks, Threats Insider attacks Lack of contingency, Poor configuration. Serangan: Passive attacks, Active attacks, Phishing, Social Engineering, Hijack Teknologi: Firewall, Antivirus, IDS,	Tujuan keamanan mencakup perlindungan informasi dan properti dari pencurian, korupsi, atau serangan ancaman, sambil memungkinkan informasi dan properti tetap dapat diakses dan produktif bagi pengguna yang dituju.
17	Nurse et al., 2014	IEEE Security and Privacy Workshops	Research Paper	Ancaman, Serangan	Kuantitatif	Ancaman: External Threats, Internal Threats. Serangan: Social engineering, SQL	K erangka kerja dapat menangkap dan mengidentifikasi sebagian besar elemen kunci yang membentuk masalah ancaman-orang

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						injection, Cross Site Scripting (XSS), Brute force attack	dalam, mulai dari peristiwa dan indikator yang signifikan (misalnya elemen perilaku dan teknis), hingga faktor manusia yang berada di belakang (bahkan tidak disengaja) serangan.
18	Pawar & Anuradha, 2015	International Conference on Intelligent Computing, Communication & Convergence	Research Paper	Serangan	Kuantitatif	Serangan: Active attacks, Passive attacks	Harus memiliki program antivirus yang diperbarui. Jangan memberikan lebih banyak atau tidak diinginkan akses ke pengguna jaringan apa pun. Sistem operasi harus diperbarui secara berkala
19	Joshi & Karkade, 2015	International Journal of Computer Science and Mobile Computing	Research Paper	Teknologi Keamanan	Kuantitatif	Teknologi: Asymmetric cryptosystems, Symmetric cryptosystems	Kriptografi, bersama dengan protokol komunikasi yang sesuai, dapat memberikan perlindungan tingkat tinggi dalam komunikasi digital terhadap serangan penyusup sejauh menyangkut komunikasi antara dua komputer yang berbeda.
20	Funmilola & Oluwafemi, 2015	Network and Complex Systems	Review Paper	Ancaman, Serangan, Teknologi Keamanan	Kualitatif	Ancaman: Insider attacks, Threats Insider attacks Lack of contingency, Poor configuration. Serangan: Passive attacks, Active attacks, Phishing, Social Engineering, Hijack Teknologi: Firewall, Antivirus, IDS	Mengetahui metode serangan, memungkinkan keamanan yang sesuai muncul. Banyak bisnis mengamankan diri mereka dari internet melalui firewall dan mekanisme enkripsi
21	Roozbahani & Azad, 2015	International Journal Advanced Networking and Applications	Research Paper	Ancaman, Teknologi Keamanan	Kuantitatif	Ancaman: Email berisi virus, virus jaringan, web-based virus, attack server. Teknologi: Cryptographic	Untuk menghadapi ancaman dan kerentanan yang ada, termasuk teknik enkripsi di mana data sederhana dienkripsi dalam teks sedemikian rupa

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						systems, Firewall, IDS, Anti-Malware Software, IPSec, SSL	sehingga sulit untuk dipahami dan ditafsirkan. Ini akan mengurangi kemungkinan intrusi jaringan. Di sisi lain teknik IDS dan IPS mengontrol pertukaran informasi dalam jaringan dan mencegah akses yang tidak sah.
22	Choubey & Hashmi, 2018	International Journal of Scientific Research in Computer Science, Engineering and Information Technology	Research Paper	Teknologi	Kuantitatif	Teknologi: Asymmetric cryptosystems, Symmetric cryptosystems	Banyak organisasi menggunakan kriptografi untuk mengamankan informasi penting tentang proyek kerjanya saat ini dimana tidak ada pihak ketiga yang dapat memengaruhi datanya

Dari Tabel 1 di atas tampak demografi item data dari 22 *paper* yang terpilih menunjukkan bahwa *paper-paper* tersebut dapat diklasifikasi menjadi beberapa buah berdasarkan isi penelitian yang terdapat pada *paper* tersebut. Secara garis besar klasifikasinya berdasarkan pada topik tinjauan yang dilakukan yaitu mengenai ancaman (A), serangan (S) dan teknologi keamanan (T). Klasifikasi detil dari 22 *paper* yang terpilih ditunjukkan pada Tabel 3.

Tabel 2. Klasifikasi *Paper*

No	Penulis	Topik		
		Ancaman (A)	Serangan (S)	Teknologi (T)
1	Singh, et. al	√	√	√
2	Stosic, et. al		√	√
3	Jouini, et. al	√		
4	Konakalla, et. al		√	√
5	Gaigole, et. al		√	√
6	Khan, et. al	√	√	√
7	Sanghavi, et. al		√	√
8	Farooq		√	√
9	Kotkar, et. al		√	√
10	Geric, et. al	√		
11	Safianu, et. al	√	√	
12	Conteh, et. al		√	√
13	Bays, et. al		√	√
14	Jain, et. al		√	√
15	Alabady		√	√
16	Bhatia, et. al	√	√	√
17	Nurse, et. al	√	√	
18	Pawar, et. al		√	
19	Joshi			√
20	Funmilola et. al	√	√	√
21	Roozbahani, et. al	√		√
22	Choubey et. al			√

Dari Tabel 2 di atas dapat diketahui bahwa kombinasi klasifikasi 22 paper yang dipilih adalah: AST (4 *paper*), ST (10 *paper*), AS (2 *paper*), AT (1 *paper*), A (2 *paper*), S (1 *paper*) dan T (2 *paper*). Banyak *paper* yang saling beririsan yaitu memuat topik tentang ancaman (A), serangan (S) atau teknologi keamanan (T) seperti pada klasifikasi AST, ST, AS dan AT.

Pemetaan

Menerapkan teknologi keamanan yang sesuai sebagai antisipasi dari beraneka ragam jenis ancaman atau serangan pada jaringan atau sistem informasi merupakan hal mutlak yang harus dilakukan organisasi dalam upaya melindungi aset informasi mereka. Melakukan pemetaan antara jenis ancaman atau serangan dengan teknologi keamanan yang ada haruslah berdasarkan pada aspek dasar dari keamanan jaringan atau sistem informasi, yaitu: kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*).

Dengan mengetahui aspek keamanan tersebut di atas, maka akan menjadi lebih mudah dalam mengidentifikasi ancaman atau serangan dan menentukan implementasi teknologi keamanan yang sesuai sebagai tindakan perlindungannya. Pemetaan antara ancaman atau serangan dengan teknologi keamanannya ditunjukkan pada Tabel 3.

Tabel 3. Pemetaan Ancaman/Serangan dengan Teknologi Keamanan

No	Aspek Keamanan	Ancaman / Serangan	Teknologi Keamanan
1	Kerahasiaan (*Confidentiality*)	*Eavesdropping* *Phishing Attacks* *Denial of Services* *Spoofing* *Hijack* *Man-in-the-Middle-Attack* *Masquerading* *Social Engineering*	*Cryptographic System* *IDS* *Firewall* *IPSec* *SSL* *Authentication*
2	Integritas (*Integrity*)	*Virus, Worm, Trojan* *Eavesdropping* *Denial of Services* *Spoofing*	*Antivirus System* *Cryptographic System* *IDS* *Firewall* *IPSec* *SSL*
3	Ketersediaan (*Availability*)	*Traffic Analysis* *Denial of Services* *Modification*	*Firewall* *IDS* *Antivirus System*

Dari Tabel 3 di atas dapat diketahui bahwa pada setiap aspek keamanan yang ada yaitu kerahasiaan, integritas dan ketersediaan, terdapat beragam ancaman atau serangan pada jaringan atau sistem informasi. Demikian pula terdapat beragam teknologi keamanan yang digunakan sebagai antisipasi dan perlindungan dari ancaman atau serangan yang ada tersebut. Terlihat bahwa *firewall*, IDS, *antivirus system* dan *cryptographic system* menjadi teknologi keamanan pilihan disebabkan kehandalan mereka dalam mengantisipasi dan melindungi jaringan atau sistem informasi pada aspek keamanan yang berbeda-beda.

IV. Kesimpulan

Dari penelitian tentang *systematic review* terkait dengan ancaman, serangan dan tindakan perlindungan pada keamanan jaringan atau sistem informasi, maka penulis menyimpulkan bahwa teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari beragam ancaman atau serangan keamanan. Agar penentuan teknologi keamanan dapat sesuai dengan kebutuhan organisasi, maka diperlukan pemetaan terlebih dahulu antara jenis ancaman atau serangan dengan teknologi keamanan yang ada berdasarkan kepada aspek keamanan, yaitu: kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*). Dengan demikian pemilihan teknologi keamanan yang sesuai dapat dilakukan serta dapat mengurangi beban biaya dikarenakan tersedianya teknologi yang memiliki beraneka ragam fungsi dan kehandalan keamanan seperti *firewall*, IDS, *antivirus system* dan *cryptographic system.*

Agar proses *systematic review* tentang ancaman, serangan dan tindakan perlindungan pada keamananan jaringan atau sistem informasi menjadi lebih baik dan lengkap, maka penulis menyarankan untuk penelitian-penelitian selanjutnya sebaiknya dapat meningkatkan jumlah paper yang akan ditinjau. Sehingga diharapkan hasil analisis yang didapat menjadi lebih variatif dan memberikan solusi yang lebih efektif dalam analisis keamanan jaringan atau sistem informasi.

DAFTAR PUSTAKA

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of E-Technology*, *1*(2), 26–36.

Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., & Mauro Madeira, E. R. (2015). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, *6*(1), 1–19. https://doi.org/10.1186/s13174-014-0015-z

Bhatia, P., & Sehrawat, R. (2014). Type of Security Threats and its Prevention. *IJSRD-International Journal for Scientific Research & Development*|, *2*(08), 2321–0613. Retrieved from www.ijsrd.com

Choubey, R. K., & Hashmi, A. (2018). Cryptographic Techniques in Information Security, *3*(1), 854–859.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Farooq, U. (2018). Network Security Challenges, (August), 2–7. https://doi.org/10.13140/RG.2.2.27478.34885

Fatemeh Soleimani Roozbahani, & Reihaneh Azad.

(2015). Security Solutions against Computer Networks Threats. *International Journal of Advanced Networking and Applications (IJANA)*, *7*(01), 2576–2581. Retrieved from http://www.ijana.in/papers/V7I-1.pdf

Funmilola, A., & Oluwafemi, A. (2015). Review of Computer Network Security System. *Network and Complex Systems*, *5*(5), 40–47. Retrieved from www.iiste.org

Gaigole, M. S., & Prof, K. M. . (2016). The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms. *Journal of Laser Applications*, *28*(3), 032007. https://doi.org/10.2351/1.4947598

Geric, S., & Zejko, H. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences*, *31*(1), 51–61.

Jain, A. K., Singh, Y., & Updhyay, S. (2012). Information systems security: A review. *Ind Jour Math & Comp Sc*.

Joshi, M. R., & Karkade, R. A. (2015). Network Security with Cryptography. *International Journal of Computer Science and Mobile Computing*, *41*(1), 201–204.

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Khan, R. (2017). Network Threats, Attacks and Security Measures: a Review. *International Journal of Advanced Research in Computer Science*, *8*(8), 116–120. https://doi.org/10.26483/ijarcs.v8i8.4641

Konakalla, A., & Veeranki, B. (2013). Evolution of Security Attacks and Security Technology. *Ijcsmc*, *2*(11), 270–276.

Kotkar, A., Nalawade, A., Gawas, S., & Patwardhan, A. (2013). Network Attacks and Countermeasures. *Information Security Management Handbook, Sixth Edition, Volume 7*, *1*(1), 21–22. https://doi.org/10.1201/b15440-4

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Journal of Clinical Epidemiology*, *62*(10), e1–e34. https://doi.org/10.1016/j.jclinepi.2009.06.006

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *Proceedings - IEEE Symposium on Security and Privacy*, *2014-Janua*, 214–228. https://doi.org/10.1109/SPW.2014.38

Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, *48*(C), 503–506. https://doi.org/10.1016/j.procs.2015.04.126

Safianu, O., Twum, F., & B., J. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications*, *143*(5), 8–14. https://doi.org/10.5120/ijca2016910160

Sanghavi, P., Mehta, K., & Soni, S. (2010). Network security. *International Journal of Scientific and Research Publications*, *1*(8), 460–464. https://doi.org/10.1201/b15107-10

Singh, S. K. S., Singh, M. P., Singhtise, D., & Singh, D. K. (2011). A survey on network security and attack defense mechanism for wireless sensor networks. *International Journal of Computer Trends and Technology*, *1*(2), 9–17. Retrieved from http://ijcttjournal.org/volume-1/issue-2/ijcttjournal-v1i2p2.pdf

Stosic, L., & Velickovic, D. (2013). Computer security and security technologies. *Journal of Process Management. New Technologies*, *1*(1), 14–19. https://doi.org/10.5937/jpmnt1301014s