urnal Manajemen USNI
Volume 9 No 2 Februari 2024 40-54
P-ISSN : 2528-7044
E-ISSN : 2809-5103
DOI:https://doi.org/10.54964/manajemen/

TANTANGAN TERKINI DALAM KEAMANAN INFORMASI ANALISIS RESIKO DAN UPAYA PERLINDUNGAN

Parida Amalia[1], Muhammad Irwan Padli Nasution[2]
Universitas Islam Negeri Sumatera Utara
Paridaamalia0@gmail.com[1], irwannst@uinsu.ac.id[2]

Received:	Accepted:	Published:
11 Desember 2023	20 Januari 2024	1 Februari 2024

ABSTRAK

Ancaman dan serangan yang dapat mengakibatkan kebocoran data pribadi atau sensitif atau penurunan kinerja bisnis berdampak signifikan terhadap keamanan jaringan dan sistem informasi. Serangan orang dalam, penyadapan, kesalahan konfigurasi, fungsionalitas yang hilang, kebingungan, serangan man-in-the-middle, serangan virus, serangan penolakan layanan adalah beberapa bahaya yang mengancam keamanan jaringan Anda atau mengancam keamanan jaringan Anda. Serangan mungkin terjadi. Mempengaruhi sistem informasi. Perusahaan berisiko kehilangan aset informasi jika tidak mengambil tindakan pengamanan yang tepat, seperti keamanan jaringan dan sistem informasi. Anda dapat menerapkan solusi keamanan yang tepat untuk memprediksi dan mencegah berbagai risiko dan serangan keamanan. Kerahasiaan, integritas, dan ketersediaan adalah tiga karakteristik keamanan, dan untuk menentukan teknologi keamanan mana yang sesuai dengan kebutuhan organisasi, pertama-tama Anda harus membandingkan berbagai ancaman dan serangan dengan teknologi keamanan yang sedang digunakan. Teknologi keamanan yang direkomendasikan mencakup firewall, sistem deteksi intrusi (IDS), program antivirus, dan sistem enkripsi. Hal ini karena teknologi ini mengandalkan prediksi dan perlindungan jaringan dan sistem informasi di banyak elemen keamanan.

Kata kunci*: *Keamanan Informasi, Analisis resiko dan Upaya Pelindungan

ABSTRACT

Threats and attacks that can result in leaks of personal or sensitive data or reduced business performance significantly impact the security of networks and information systems. Insider attacks, eavesdropping, misconfiguration, missing functionality, confusion, man-in-attacks, virus attacks, and denial of service attacks are some of the dangers that threaten your network security or the security of your network. Attacks are possible. Influencing information systems. Companies risk losing information appropriate security measures, such as network and information system security. You can implement the right security solutions to predict and prevent various security risks and attacks. Confidentiality, integrity, and availability are three characteristics of security, and to determine which security technology best suits your organization's needs, you must first compare the various threats and attacks with the security technologies in use. Recommended security technologies include intrusion detection systems (IDS), antivirus programs, and encryption systems. This technology predicts and protects networks and information systems in many security elements.

***Keywords:** Information Security, Risk Analysis and Protection Efforts*

PENDAHULUAN

Pesatnya ekspansi industri teknologi informasi telah meningkatkan transfer data dan informasi di seluruh dunia. Manfaat nyata dari teknologi informasi diimbangi oleh tingginya risiko penyalahgunaan dan risiko yang kompleks.Organisasi semakin rentan terhadap risiko dan serangan terkait keamanan jaringan atau informasi yang diakibatkan oleh berbagai operasi internal dan serangan peretas (Rabi, Aissa, dan Ouini, 2014).

Ada berbagai jenis serangan yang dapat membahayakan operasi dan layanan perusahaan, termasuk: Contoh: serangan orang dalam, sistem yang tidak dikonfigurasi dengan benar, kurangnya rencana cadangan, pencurian identitas, serangan man-in-the-middle, serangan virus, serangan penolakan layanan, dll.

Bhatia dan Sehrawat, Nurse et al. Pathar dan Anuradha et.al. Veeranki dan Konakalla (2015). Organisasi berisiko kehilangan aset informasinya jika tindakan keamanan yang tepat tidak diambil, termasuk keamanan jaringan dan sistem informasi. Proses menjaga sumber daya informasi yang dilindungi, termasuk ketersediaan, kerahasiaan, dan integritasnya, disebut keamanan jaringan sistem informasi. (Alabady, 2009).

Aturan dan prosedur yang dikenal sebagai pengamanan jaringan atau sistem informasi digunakan untuk memantau dan mencegah akses tidakk dapat dentifikasi, memodifikasi sistem, penyalahgunaan, dan akses yang ditolak ke jaringan komputer dan sumber daya yang dapat diakses melalui jaringan (Pawar & Anuradha, 2015). Menurut Farooq (2018). Untuk melindungi sumber daya informasi dari pengancaman dan serangan sistem informasi, pengenalan teknologi keamanan merupakan salah satu pilihan. Berbagai solusi keamanan tersedia untuk melindungi jaringan dan sistem informasi dari ancaman dan serangan, termasuk firewall, sistem enkripsi, IDS, SSL, sistem antivirus, IPSec, dan otentikasi. (Veeranki dan Konakalla et.al Prof & Gaigole, et.al Khan, et.al Sanghavi, Mehta & Soni 2017)

Masalah dengan penelitian terbatas yang menghubungkan ancaman jaringan atau sistem informasi saat ini serta teknik peengamanan yang tepat sebagai tindakan pengendalian adalah pertanyaan yang muncul dari penelitian yang dilakukan. Untuk memastikan bahwa pemetaan berguna untuk penelitian di masa depan, proyek ini akan melakukan tinjauan komprehensif terhadap penelitian yang dipublikasikan mengenai risiko, serangan, dan penanggulangan keamanan jaringan atau sistem informasi.

Tinjauan sistematis ini tidak mendefinisikan metode analisis tertentu, juga tidak memberikan evaluasi terhadap analisis penelitian sebelumnya yang sudah ada.

RQ: Implementasi teknologi keamanan manakah yang tepat untuk memprediksi jenis serangan pada jaringan dan sistem informasi?

Keenam komponen pembahasan meliputi pengembangan tinjauan sistematis dan persiapan untuk menyajikan hasilnya. Bagian 1 adalah pendahuluan. Bagian 2 adalah metode. Bagian 3 adalah hasil dan pembahasan. Dan bagian 4 adalah kesimpulannya.

KAJIAN LITERATUR

Menurut Farooq (2018). Untuk melindungi sumber daya informasi dari pengancaman dan serangan melalui jaringan dan sistem informasi, pengenalan teknologi pengamanan adalah salah satu pilihan. Berbagai solusi keamanan tersedia untuk melindungi jaringan dan sistem informasi dari ancaman dan serangan, termasuk firewall, sistem enkripsi, IDS, SSL, sistem antivirus, IPSec, dan otentikasi.

METODE PENELITIAN

Kriteria pelaporan untuk PRISMA (Item Pelaporan Pilihan untuk Tinjauan Sistematis dan Meta-analisis) diikuti dalam persiapan tinjauan sistematis ini (Liberati et al., 2009). Ada beberapa prosedur. Mengikuti rekomendasi ini, khususnya, penelitian ini:

- Persyaratan kelayakan,
- sumber informasi,
- pilihan studi,
- pengambilan data,
- pemilihan data semuanya ditentukan.

1. Kriteria kelayakan

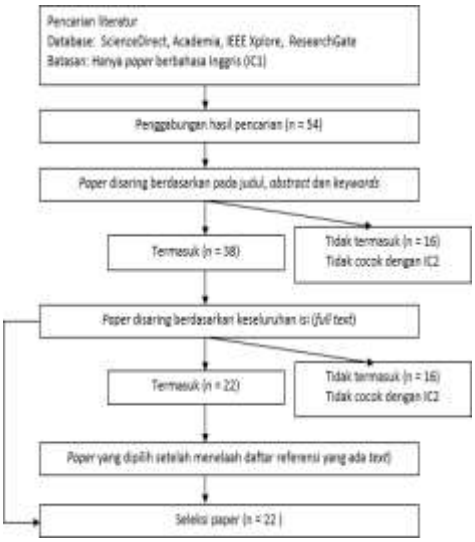
Prosedur peninjauan untuk kriteria inklusi (IC) berikut telah ditetapkan:

IC1: Penelitian asli berbahasa Inggris yang telah menjalani peer review;

IC2: Penelitian pengamanan jaringan atau sistem informasi dengan tujuan mendeteksi risiko dan menempatkan teknologi keamanan di tempat sebagai tindakan pencegahan.

Karena bahasa *Inggris* merupakan bahasa utama yang digunakan oleh para ilmuwan, hanya artikel yang diterbitkan dalam bahasa *Inggris* (IC1) yang terpilih. Untuk menanggapi pertanyaan penelitian, IC2 ditambahkan.

Penulis tertarik pada berbagai topik, tidak hanya ancaman sistem informasi dan teknologi keamanan. Ancaman mungkin dapat mengganggu kinerja dan layanan organisasi adalah bidang lain yang menarik bagi penulis. Upaya penulis dalam melakukan tinjauan sistematis dijelaskan pada Gambar 1, yang merupakan diagram aliran PRISMA.



Gambar 1. *Diagram Alir PRISMA*

2. Sumber informasi

Sumber daya penelitian akademis seperti Science Direct, Academia, IEEE Xplore, dan ResearchGate memberi kami artikel yang kami butuhkan untuk melakukan penelitian sistematis. Tidak ada kriteria; Penulis hanya mengakses artikel dalam upaya untuk mendapatkannya. Para penulis juga melihat-lihat daftar referensi makalah untuk menemukan penelitian terkait.

3. Pemilihan studi

Tahap-tahap berikut digunakan untuk memilih studi :

1) Untuk mengevaluasi risiko dan serangan terhadap pengemanan jaringan dan sistem informasi, serta teknik keamanan dengan tindakan pencegahan, penulis memilih kata kunci untuk pencarian kata kunci berdasarkan minat penelitiannya.“Keamanan jaringan”, “serangan dan perlindungan keamanan”, “keamanan informasi”, dan “ancaman, serangan, dan teknologi keamanan” adalah kata kunci yang digunakan saat mencari artikel di database untuk **Bagian II.B.**

2) Kriteria seleksi digunakan sebagai pedoman pencarian judul, abstrak, dan kata kunci publikasi dan sudah teridentifikasi.

3) Untuk memastikan apakah suatu karya dapat diterima untuk ditinjau, karya tersebut dibaca seluruhnya atau sebagian jika memenuhi persyaratan.

4) Studi yang relevan ditemukan dengan melihat melalui daftar referensi publikasi.

Masing-masing penulis yang melakukan tinjauan sistematis ini bekerja sama untuk menyelesaikan langkah-langkah yang disebutkan di atas. Jika terjadi perselisihan, pembicaraan berlanjut sampai solusi yang dapat diterima bersama ditemukan.

4. Pengumpulan data

Pengumpulan data manual dilakukan dengan alat tabel ekstraksi data yang meliputi hal-hal berikut: judul, penulis, tahun, nama publikasi atau konferensi, jenis makalah, topik, metodologi studi, hasil diskusi, dan kesimpulan. Makalah yang berpotensi atau sudah relevan dievaluasi bersama. Membaca seluruh buku dan mengekstraksi data merupakan evaluasi. Para penulis berkomunikasi dan mencari tahu perbedaan apa pun.

5. Pemilihan item data

Data yang diproleh dari masing-masing artikel terdiri dari: a) Uraian mengenai keamanan jaringan serta sistem informasi.b) Risiko Serangan Keamanan. c) Gunakan teknologi pengamanan terkini untuk keamanan.

HASIL DAN PEMBAHASAN

Pada tahun 2009 sampai 2019 ada 54 artikel yang diterbitkan dalam bahasa *inggris* yang serasi dengan istilah pencarian penting diperiksa ditemukan dalam hasil pencarian database yang dipilih. Makalah kemudian disaring lebih lanjut menggunakan kata kunci, abstrak, dan judul. Setelah meninjau 38 artikel yang tersisa menggunakan seluruh teks, hingga 16 dari mereka didiskualifikasi karena gagal memenuhi persyaratan IC2. Total 22 publikasi yang memenuhi persyaratan kelayakan dimasukkan sebagai bahan dalam tinjauan sistematis ini.

Karakteristik *paper*

Tabel 1 tentang ekstraksi data akhir memberikan informasi rinci dari 22 studi yang dipilih. Ekstraksi data terakhir adalah tabel ekstraksi data yang hanya mencakup makalah yang dipilih sesuai dengan kriteria prosedur pemilihan makalah (Bagian Tiga. A).

Tabel 1. Ekstrasi Data Final

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
1	Singh et al., 2011	International Computer Trends and Technology Journal	Examine this paper	Teknologi Keamana, Serangan, dan Ancaman	Kualitatif	Ancaman: Serangan dari luar sebagai lawan dari dalam, Perbandingan antara serangan pasif dan agresif serangan menggunakan kelas notebook ayat kelas mote. Serang: Gangguan, keterlambatan layanan, Sybil, Wormhole, dan Blackhole. Teknologi: LEAP, TinySec, dan SPIN	Keamanan pada WSN akhir-akhir ini mendapat banyak perhatian. Karena karakteristik khusus WSN, sangat sulit untuk menciptakan mekanisme keamanan yang kuat dengan sedikit usaha.
2	Stosic and Velickovic (2013)	Jurnal Manajemen Proses: Emerging Technologies	Review Article	Serangan Siber, TeknologiKeamanan	Kualitatif	Serangan: Dimodifikasi, Dibuat, Memotong atau melanggar, Intersepsi. Technolog: verifikasi dan enkripsi. Pemberian izin	Serangan termasuk melewati atau menghancurkan, menciptakan, mencegat, dan mengubah. Teknologi: Otentikasi dan enkripsi. izin

3	Jouini and colleagues (2014)	Kemajuan dalam Ilmu Komputer	Sebua makalah penelitian	Ancaman	Kuantitatif	Ancaman: Bahaya dari Luar dan Dalam	Untuk lebih memahami risiko keamanan, disajikan model untuk mengklasifikasikan ancaman keamanan. Karena ancaman berubah seiring waktu, model ini memungkinkan Anda mengeksplorasi dampak dari berbagai kelas ancaman.
4	Konakalla and Veeranki (2013)	Jurnal Ilmu Komputer dan Mobile Computing International	Panduan Belajar	Serangan Siber, Teknologi Keamanan	Kuantitatif	Metode serangan termasuk Trojan horse, hacking, worm, serangan DoS, virus, dan infectors dari sistem dan boot record. Teknologi termasuk IPSec, SSL, firewall, sistem deteksi intrusi, dan perangkat lunak pencegahan malware.	Keamanan cukup penting dan harus dijaga supaya pengguna Internet mampu berpartisipasi dalam aktivitas online dengan percaya diri.
5	Gaigole > Prof, 2016	Jurnal Ilmu Komputer dan Mobile Computing International	Research Paper	Serangan Siber, Teknologi Keamanan	Kuantitatif	Jenis serangan termasuk terdistribusi, aktif, dan pasif. Teknologi termasuk IPSec, SSL, firewall, sistem deteksi intrusi, dan perangkat lunak pencegahan malware.	Dengan banyaknya kekayaan intelektual yang tersedia secara online, keamanan jaringan sangatlah penting.jenis- jenis serangan bisa terjadi ketika informasi dikirimkan melalui jaringan. Dengan memahami teknik serangan, Anda dapat membangun pengamanan akurat. Firewall dan alat enkripsi adalah alat umum yang digunakan bisnis untuk melindungi diri mereka secara online.

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
6	Khan, 2017	Jurnal Internasional Penelitian Lanjutan dalam Ilmu Komputer	Review Paper	Ancaman, Serangan, Teknologi Keamanan	Kualitatif	Ancaman: Serangan orang dalam, Ancaman Serangan orang dalam Kurangnya kemungkinan, Konfigurasi buruk. Serang: Serangan pasif, Serangan aktif, Phishing, Rekayasa Sosial, Pembajakan Teknologi: Firewall, Antivirus, IDS,	There are many types of threats and attacks against network systems, and there are also common precautions to mitigate adverse situations.
7	Sanghavi et al., 2010	Jurnal Internasional Publikasi Ilmiah dan Penelitian	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serang: Menguping, Virus, Worm, Trojan, Phishing, IP Spoofing, DoS. Teknologi: Sistem kriptografi, Firewall, IDS, Antimalware, SSL,	The combined use of firewalls, intrusion detection, and authentication mechanisms will likely prove effective in protecting intellectual property shortly. The field of network security may need to evolve more quickly to address additional threats in the future
8	Farooq, 2018	Jurnal Internasional Penelitian Lanjutan dalam Ilmu Komputer	Research Paper	Serangan,Teknologi Keamanan	Kuantitatif	Serangan: Serangan aktif, Serangan pasif Teknologi: Firewall, Kriptografi, SSL, IDS, Antivirus	Many companies and governments take many measures to maintain privacy and security and prevent cyber attacks, but cyber security is still a big concern.
9	Kotkar et al., 2013	Jurnal Internasional Penelitian Inovatif dalam Teknik Komputer dan Komunikasi	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serang: MAC Flooding, Pembajakan, IP Spoofing, DoS Teknologi: IEEE 802.1X suites, Enkripsi, Otentikasi, Firewall, IDS	Ethical hackers can do to the network if the network is weak
10	Geric & Zejko, 2007	Jurnal Internasional Publikasi Ilmiah dan Penelitian	Research Paper	Ancaman	Kuantitatif	Ancaman: Kesalahan dan kelalaian, Penipuan dan pencurian, Karyawan sabotase	The existing classification is outdated, especially in the context of its compatibility and comparability.

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						Hackers, Malware	Model C3 Ciri utamanya ialah fleksibel, dinamis, dan multidimensi, sehingga memberikan kelebihannya dari model klasifikasi lain yang tertera di atas..
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	Pengamanan informasi tidak bisa dijelaskan dengan masalah teknis saja. Karena komputer dioperasikan manusia, informasi bisa mennjadi masalah bagi manusia. Oleh karena itu, untuk membatasi pelanggaran informasi dan data, organisasi didorong untuk mengadopsi kerangka pengamanan komprehensif.
12	Conteh & Schmick, 2016	International Journal of Advanced Computer Research	Research Paper	Serangan, Teknologi Keamanan	Kuantitatif	Serangan: Social engineering Teknologi: IDS, IPS, Firewall	Teknologi dapat berperan dalam memitigasi akibat serangan secara sosial. Kerentanannya terletak dalam perilaku manusia, dorongan hati cendrung psikologis yang dipengaruhi oleh yang lain.

13	Bays et al., 2015	Journal of Internet Services and Applications	Research Paper	Ancaman, Teknologi Keamanan	Kuantitatif	Ancaman: Information leakage, Identity fraud, Physical resources overloading. Teknologi: Access control, Authentication, Cryptography, Firewall	Diperlukan juga agar bisa melindungi infrastruktur jaringan virtual Anda dan membuatnya dapat digunakan di lingkungan nyata.

No	Penulis	Nama Jurnal/ Conference	Type 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	Kemajuan teknologi meningkatkan kompleksitas sertamempertajam kurva pembelajaran. Kompleksitas menyebabkan pengawasan dan kesenjangan 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 memberi control jaringan dan lalu lintas, serta melakukan otentikasi router yang sama dan memberikan keamanan yang lebih baik daripada hanya hanya satu saja. Pengaturan pemfilteran router yang tidak memadai dapat mengurangi pengamanan jaringan secara keseluruhan dan membuat komponen system informasi internal rentan terhadap pemindaian serta 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,	Sasaran pengamanan meliputi melindungi informasi seperti properti dari pencurian, kerusakan, atau ancaman sekaligus memastikan bahwa pengguna yang ditargetkan dapat mengakses informasi dan properti mereka dan tetap produktif.
17	Nurse et al., 2014	IEEE Security and Privacy Workshops	Research Paper	Ancaman, Serangan	Kuantitatif	Ancaman: External Threats, Internal Threats. Serangan: Social engineering, SQL	Kerangka pengerjaan bisa mengidentifikasi pada berbagai elemen kunci dan membentuk suatu permasalahan. pemerasan

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						injection, Cross Site Scripting (XSS), Brute force attack	Dimulai dari indikator penting (seperti faktor sifat dan teknis) hingga factor dibalik serangan (bahkan yang tidak disengaja).
18	Pawar & Anuradha, 2015	International Conference on Intelligent Computing, Communication & Convergence	Research Paper	Serangan	Kuantitatif	Serangan: Active attacks, Passive attacks	Menyimpan daftar antivirus terbarukan. Tidak menyerahkan lebih dari yang diinginkan akses ke pemakai. Sistem penggunaan bisa diperbarui berkala

19	Joshi & Karkade, 2015	International Journal of Computer Science and Mobile Computing	Research Paper	Teknologi Keamanan	Kuantitatif	Teknologi: Asymmetric cryptosystems, Symmetric cryptosystems	Kriptografi, berikut pakai pewara relasi yang sesuai, bisa memasrahkan dukungan taraf tinggi bagian dalam relasi digital terhadap gempuran penyelundup sebelit mencantol relasi renggangan 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	Bagaimana susunan serangan, memungkinkan ketenangan yang setuju muncul. Banyak niaga menyergap selira mencari akal berusul internet menelusuri 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	Memerangi serangan serta mudah datanng serta menggabungkan teknik enkripsi data menjadi teks seperti biasa

No	Penulis	Nama Jurnal/ Konferensi	Tipe Paper	Topik	Metode	Hasil Pembahasan	Kesimpulan
						systems, Firewall, IDS, Anti-Malware Software, IPSec, SSL	Cukup susah memang dipahami dan ditafsirkan. dan kemungkinan intrusi jaringan. Teknik IDS dan IPS menngawasi 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	Rata-rata organisasi menggunakan kriptografi melindungi informasi sensitif mengenai proyek kerja, mencegah pihak ketiga mempengaruhi data.

Dari Tabel 1 di atas, elemen data demografi dari 22 *paper* serta dipilih akan memberitahu bahwa *paper* tersebut diklasifikasikan ke dalam kategori sesuai dengan konten penelitian dimuat dalam *paper*. Umumnya klasifikasi didasarkan pada tema review yang dibuat: ancaman (A), serangan (S), dan teknologi keamanan (T).

Klasifikasi rinci dari 22 makalah 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.	√	√	

No	Penulis	Topik		
		Ancaman (A)	Serangan (S)	Teknologi (T)
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, mengkombinasi klasifikasi dari 22 makalah terpilih adalah AST (4 makalah), ST (10 makalah), AS (2 makalah), AT (1 makalah), dan A (2 makalah).), S (1 karangan), T (2 karangan). Bnayak esai tumpang tindih dan mencakup topik yang berkaitan dengan ancaman (A), serangan (S), atau teknologi keamanan (T), seperti klasifikasi AST, ST, AS, dan AT.

Pemetaan

Agar organisasi dapat melindungi aset informasinya, sangat penting bagi mereka untuk menerapkan teknologi keamanan yang tepat yang mengantisipasi jenis pengancaman dan serangan terhadap sistem informasi. Asosiasi serangan dengan teknologi pengamanan timbul harus didasarkan pada aspek fundamental pengamanan sistem informasi: kerahasiaan, integritas, dan ketersediaan. Aspek pengamanan di atas memudahkan dalam mengidentifikasi ancaman dan serangan serta memutuskan penggunaan teknologi keamanan yang tepat untuk sarana perlindungan. Hubungan ancaman atau serangan keamanan diperlihatkan 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	Integrity as (*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, terdapat beberapa peerbedaan ancaman dan serangan terhadap jaringan atau sistem informasi di setiap aspek pengamanan: kerahasiaan, integritas, dan ketersediaan. Ada juga berbagai teknologi keamanan yang digunakan untuk memprediksi dan mencegah ancaman dan serangan yang ada. Firewall, IDS, sistem antivirus, dan sistem enkripsi terbukti teknologi keamanan pilihan karena keandalannya saat memprediksi dan menjaga sistem informasi dalam berbagai aspek keamanan.

SIMPULAN

Dari penelitian mengenai tinjauan sistematis terkait ancaman, serangan, dan tindakan pengamanan sistem informasi, penulis dapat memprediksi berbagai ancaman dan serangan keamanan serta mengembangkan teknologi keamanan yang tepat untuk melindunginya.
Untuk menentukan teknologi keamanan sesuai kebutuhan organisasi Anda, pertama-tama Anda perlu memetakan jenis pengancaman serta serangan dengan teknologi pengamana harus berdasarkan aspek keamanan: kerahasiaan, integritas, dan ketersediaan.

Melalui cara ini, ketersediaan teknologi dengan beragam fitur dan keandalan keamanan, misalnya firewall, IDS, sistem antivirus,serta sistem enkripsi, memungkinkan pemilihan teknologi keamanan yang sesuai dan pengurangan biaya.Agar proses tinjauan sistematis terkait ancaman, serta perlindungan pada keamanan sistem informasi akan lebih tepat dan terpenuhi jumlahnya, penulis akan menambah jumlah artikel yang diulas pada penelitian selanjutnya, saya menyarankan hal tersebut perlu dilakukan. Oleh karena itu, hasil analisis yang diperoleh akan beragam serta memberi solusi lebih efektif untuk analisis keamanan jaringan dan sistem informasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan rasa terimakasi Tuhan Yang Maha Esa dimana berkat bantuannya penulis dapat menyelesaikan artikel ini. Terimakasih juga kepada seluruh pihak yang ikut berkontribusi dalam penulisan artikel ini hingga artikel terebut dapat terselesaikan tepat pada waktunya.

DAFTAR PUSTAKA

Alabady, S. (2009). Design and Implementation of a Network Security Model for a Cooperative Network. *International Arab Journal of 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 their 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.2016.623006Farooq, U. (2018). Network Security Challenges, (August), 2–7.

https://doi.org/10.13140/RG.2.2.27478.34885 Fatemeh Soleimani Roozbahani, & Reihaneh Azad.