Jurnal Jaringan Komputer dan Keamanan
JJKK, Vol. 04, No. 03, October 2023: 30-34
Received: 5 Mar 2020; Revised: 29 Mar 2020; Accepted: 30 Mar 2020

# Literature Review Network Security

**Muhammad Irdian Saputra**
Program Magister Teknik Informatika
Universitas Bina Darma
email :mirdiansaputra@student.binadarma.ac.id
Jl. A. Yani No. 12, Palembang 30624, Indonesia

***Abstract***

*Network security is an important aspect in today's digital era. This literature review provides a thorough overview of the technologies and methods used to protect networks from various security threats. This research explores various literature sources, including scientific articles, journals, books, and recent publications, to identify trends and current practices in the field of network security. The review begins by examining the basic concepts of network security, including identification of potential network threats, risks, and vulnerabilities. Next, encryption technologies and network security protocols such as SSL/TLS, IPsec, and VPN are explored to highlight ways to protect data in transit and at rest. In addition, this review discusses the use of firewalls, IDS (Intrusion Detection System), and IPS (Intrusion Prevention System) as a proactive network defense. Several authentication methods, including the use of strong, multi-factor passwords and prudent access policies, were also reviewed to protect the network from unauthorized access. This review also covers various open-source network security software, such as pfSense, Snort, and Suricata, which provide cost-effective alternatives for managing network security. Furthermore, an analysis of regulatory and legal compliance relevant to network security is also introduced to realize the importance of complying legal regulations and face potential sanctions resulting from data breaches. Finally, this review presents views on the importance of an integrated approach to network security, integrating technology, personnel training, strict policies, and continuous monitoring. In conclusion, this literature review provides a comprehensive overview of various aspects of network security. It is hoped to provide guidance for network security practitioners and organizations to improve their network protection and respond to the evolving security threat landscape.*

***Kata kunci:*** *Network security, encryption technology, network security protocols*

***Abstrak***

*Keamanan jaringan merupakan salah satu aspek penting dalam era digital saat ini. Literature review ini menyajikan tinjauan menyeluruh tentang teknologi dan metode yang digunakan untuk melindungi jaringan dari berbagai ancaman keamanan. Penelitian ini menggali berbagai sumber literatur, termasuk artikel ilmiah, jurnal, buku, dan publikasi terkini, untuk mengidentifikasi tren dan praktik terkini dalam bidang keamanan jaringan. Tinjauan dimulai dengan memeriksa konsep dasar keamanan jaringan, termasuk identifikasi potensi ancaman, risiko, dan kerentanan jaringan. Selanjutnya, teknologi enkripsi dan protokol keamanan jaringan seperti SSL/TLS, IPsec, dan VPN dieksplorasi untuk menyoroti cara-cara perlindungan data dalam transit dan saat beristirahat. Selain itu, tinjauan ini membahas tentang penggunaan firewall, IDS (Intrusion Detection System), dan IPS (Intrusion Prevention System) sebagai pertahanan jaringan yang proaktif. Beberapa metode autentikasi, termasuk*

*penggunaan kata sandi kuat, multi-faktor, serta kebijakan akses yang bijaksana, juga dikaji untuk melindungi jaringan dari akses yang tidak sah. Tinjauan ini juga mencakup berbagai perangkat lunak keamanan jaringan open-source, seperti pfSense, Snort, dan Suricata, yang memberikan alternatif kost-effektif untuk mengelola keamanan jaringan.Selanjutnya, analisis peraturan dan kepatuhan hukum yang relevan dengan keamanan jaringan juga diperkenalkan untuk menyadari pentingnya mematuhi peraturan hukum dan menghadapi sanksi potensial yang diakibatkan oleh pelanggaran data. Akhirnya, tinjauan ini menyajikan pandangan tentang pentingnya pendekatan terpadu dalam keamanan jaringan, mengintegrasikan teknologi, pelatihan personel, kebijakan yang ketat, dan pemantauan yang terus-menerus.Kesimpulannya, literatur review ini menyajikan gambaran komprehensif tentang berbagai aspek keamanan jaringan. Diharapkan dapat memberikan panduan bagi praktisi keamanan jaringan dan organisasi untuk meningkatkan perlindungan jaringan mereka dan menanggapi perubahan lanskap ancaman keamanan yang terus berkembang.*

***Kata kunci:*** *Keamanan jaringan, teknologi enkripsi, protokol keamanan jaringan*

## 1. PENDAHULUAN

Perkembangan teknologi dalam jaringan komputer lambat laun semakin pesat seiring dengan meningkatnya kebutuhan akan akses jaringan yang efisien, stabil dan cepat serta kemanan yang handal. Terdapat banyak informasi dalam industri yang sifatnya sangat rahasia, karena ini informasi tidak dapat dipahami oleh orang yang tidak relevan, jika tidak maka akan menyebabkan kerugian yang tidak dapat diperbaiki. Tepatnya karena tingginya rahasia informasi komputer sehingga beberapa orang yang berniat jahat memiliki ide untuk melakukan kejahatan dan selalu berharap untuk mendapatkan beberapa manfaat dari kerentanan keamanan jaringan komputer. Jaringan komputer teknologi keamanan terus berkembang, dan teknologi kriminal dari para penjahat ini juga terus menerus berkembang [1][2].

Bsahkan beberapa teknologi kriminal lebih tinggi dari level ahli komputer, sehingga jaringan keamanan tidak bisa dijamin. Karena bukti dalam proses kejahatan komputer sulit untuk dipahami, komputer kejahatan keamanan jaringan semakin sering terjadi [3][4]. Ada hal penting yang perlu dilakukan yaitu melakukan pekerjaan dengan baik dalam pencegahan keamanan jaringan komputer, untuk meminimalkan kemungkinan terjadinya kejahatan komputer. Keamanan jaringan komputer tidak terdiri dari satu aspek, tetapi mengandung empat tautan penting: perangkat lunak, perangkat keras jaringan, layanan Internet of Things dan sumber daya bersama. Menurut definisi komputer keamanan jaringan oleh Organisasi Internasional untuk Standardisasi, keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer agar tidak dihancurkan, diubah, atau lubang keamanan karenaalasan kecelakaan atau berbahaya, sehingga sistem komputer terus beroperasi dengan handal, serta layanan komputerjuga teratur [5].

Kebutuhan akan jaringan komputer semakin bertambah penting, baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan ataupun adanya peretas yang dapat mematikan sumber daya pada server. Maka dari itu perlu adanya pengamanan jaringan computer untuk mencegah adanya cyber crime. Keamanan jaringan merupakan aspek terpenting sebuah sistem dalam menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunaanya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Dalam hal ini diperlukan pengaturan jaringan computer yang baik guna memaksimalkan proses pertukaran informasi dan mengamankan dari pihak yang tidak bertanggung jawab seperti hacker [6].

## 2. METODOLOGI PENELITAN

Penelitian ini menggunakan metode Literature Review merupakan salah satu tinjauan sistematis yang dapat digunakan untuk menginterpretasikan hasil dengan berbasis bukti. Adapun langkah-langkah dalam penyusunan literature review yaitu : 1) Mengidentifikasi pertanyaan literature review, 2) Mengidentifikasi artikel yang relevan, 3) seleksi artikel, 4) Data charting, 5) Menyusun, meringkas dan melaporkan hasil [11][12].

## 3. HASIL DAN PEMBAHASAN

Keamaan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalahgunaan informasi Internet of Things, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer.

Pertama Kesalahan Informasi Internet of Things. Biasanya, dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs web dan mengunduh gambar, file, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap computer [7].

Kedua serangan pada layanan latar belakang, serangan latar belakang berupa penolakan layanan yang disebut adalah bahwa pengguna sengaja menunda atau secara ilegal menunda layanan jaringan dalam proses mengunjungi situs web atau mengunduh file seperti biasa, sehingga menyebabkan kerusakan tertentu pada keamanan jaringan komputer. Ketiga kehancuran integritas keamanan jaringan komputer, peretas atau orang lain yang tidak mematuhi kode etik dengan sengaja menggunakan berbagai cara ilegal untuk menghancurkan keamanan jaringan komputer, sehingga memengaruhi integritas keamanan komputer. Keempat memberitahukan informasi komputer, ketika informasi dalam jaringan komputer ditransmisikan secara langsung ke entitas yang tidak sahtanpa izin dari pengguna, maka sudah pasti informasi menjadi rentan. Bentuk umum dari informasi komputer yang rentan karena ada lubang tersebut termasuk aspek-aspek berikut: intrusi virus atau Trojan horse ke komputer, kerentanan sistem pengguna sendiri,penyadapan frekuensi gelombang radio pada informasi komputer, pemasangan peralatan pemantauan, pengamanan jaringan computer [8].

Sistemasi yang dipergunakan dalam melindungi sebuah jaringan dari ragam ancaman dari luar yang dapat menyebabkan rusaknya jaringan serta mengantisipasi terjadinya data perusahaan dicuri Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (Komputer desktop, laptop, smartphone, PC, tablet) dan perangkat penghubung. Selain itu, jaringan komputer adalah interkoneksi antara 2 komputer autonomous atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless). Autonomous adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh. Sehingga dapat membuat computerlain. Restars, shutdows, kehilangan file atau kerusakan system [8]. Teknologi pertahanan virus adalah tindakan pencegahan penting untuk keamanan jaringan komputer. Kekuatan dari virus perlu diperhitungkan, kerusakan yang disebabkan oleh virus pada jaringan tidak bisa dihitung. Beberapa virus dapat diisolasi dari komputer melalui pertahanan efektif, tetapi beberapa virus yang lebih parah tidak dapat sepenuhnya dihilangkan melalui beberapa jarring pelindung.

Teknologi komputer terus diperbarui dan dikembangkan, tapi peretas dan penjahat juga terus-menerus belajar, jadi kita tidak boleh berhenti mempelajari perkembangan jaringan komputer teknologi keamanan. Teknologi pelindung harus lebih cepat dari pada kecepatan para penjahat komputer mempelajari virus. Teknologi Enkripsi Data, seperti disebutkan sebelumnya, lubang keamanan informasi adalah salah satu masalah yang paling sering disebutkan dalam jaringan komputer keamanan. Dengan menggunakan teknologi enkripsi data, maka informasi pengguna tidak mudah dicuri. Enkripsi data merupakan teknologi yang mengacu pada penggunaan teknologi pemrosesan data khusus untuk menyembunyikan atau mengkhususkan data, yang melaluinya jaringan komputer, pengguna mungkin tidak memahami informasinya. Enkripsi data dapat dibagi menjadi dua bentuk: enkripsi kunci publik dan enkripsi kunci pribadi. Enkripsi kunci publik lebih aman daripada enkripsi kunci pribadi, dan itu berkembang relative terlambat. Enkripsi kunci pribadi dapat dibagi menjadi dua proses: enkripsi dan dekripsi Enkripsi dan proses dekripsi berhubungan satu sama lain, yang memiliki efek perlindungan tertentu pada keamanan informasi. Enkripsi kunci pribadi tidak dibatasi oleh pengguna, siapapun dapat mengatur dan menggunakannya. Dalam hal kecepatan dekripsi, enkripsi kunci lebih cepat dari pada enkripsi kunci publik dan lebih mudah diterapkan dalam kehidupan.

Membandingkan karakteristik kriptografi kunci publik dan kriptografi kunci pribadi, dengan menemukan bahwa memiliki kelebihannya sendiri. Secara private, jika enkripsi public key dan enkripsi private key dapat digunakan bersama-sama, efek enkripsi data harus lebih tinggi [9]. Kontrol akses merupakan fitur paling penting dari kontrol akses adalah untuk memverifikasi identitas pengguna yang mengakses sumber daya komputer. Dibutuhkan audit, verifikasi otorisasi, kata sandi, kunci, dan metode otentikasi lainnya untuk melindungi pengguna keamanan informasi dan komputer. Sederhananya, ide inti dari control akses adalah bahwa informasi hanya terbuka pengguna yang benar-benar membutuhkannya dan bahwa pengguna yang masuk secara ilegal dicegah. Kontrol akses merupakan sarana penting untuk melindungi keamanan jaringan komputer.

Karena hal ini memiliki efek yang baik pada intrusi hacker. Diharapkan bahwa akan ada perkembangan penelitian yang signifikan di masa yang datang. Teknologi Firewall, Firewall merupakan teknik keamanan untuk melindungi keamanan komputer dan mencegah kegagalan komputer, juga termasuk jenis Tindakan keamanan komputer yang paling umum digunakan. Firewal dapat berupa perangkat keras, perangkat lunak, atau antara dua komputer atau lebih. Firewall dapat memberikan peran yang lebih substantif dalam melindungi komputer, karena semua aliran data perlu disaring melalui firewall. Secara umum, firewall memiliki fungsi berikut ini, fungsi pertama, firewall dapat mencegah orang lain yang tidak terkait memasuki komputer pribadi pengguna; fungsi kedua, bahkan jika seseorang dari luar memasuki sistem, maka firewall dapat mencegahnya mendekati fasilitas pertahanan; ketiga, firewall dapat mencegah mengunjungi situs khusus tertentu karena kemampuannya memfilter alamat yang tidak dikehendaki dan pada akhirnya, firewall dapat mencegah mengunjungi situs tertentu. Pada intinya komputer harus menyediakan pemantauan keamanan [10].

## 4. KESIMPULAN

Berdasarkan hasil studi literatur yang dapat diberikan informasi yaitu Keamanan jaringan komputer adalah masalah yang harus diperhatikan oleh setiap pengguna komputer. Harus diperhatikan perlunya melakukan pembersihan situs-situs phishing, tautan ilegal, spam dan sebagainya dalam komputer. Jangan pernah memberikan kesempatan kepada penjahat karena hal itu merupakan kelalaian yang bisa berdampak serius terhadap kemanan komputer. Selain itu, pengembangan teknologi keamanan jaringan komputer harus terus menerus dilakukan sesegera mungkin dan mengurangi elemen ilegal secara teknis. Masih ada jalan panjang yang harus ditempuh untuk perkembangan teknologi keamanan jaringan komputer dimasa depan. Berbagai

terobosan teknis harus direalisasikan sebagai sesegera mungkin, dan langkah-langkah perlindungan keamanan juga harus ditingkatkan.

**Referensi**


[1]. Negara, E. S. (2021). Smart Goverment.
[2]. Kaunang, F. J., Karim, A., Simarmata, J., Iskandar, A., Ardiana, D. P. Y., Septarini, R. S., ... & Widyastuti, R. D. (2021). *Konsep Teknologi Informasi*. Yayasan Kita Menulis.
[3]. Negara, E. S., Romindo, R., Tanjung, R., Heriyani, N., Simarmata, J., Jamaludin, J., ... & Purba, B. (2021). *Sistem Informasi Manajemen Bisnis*. Yayasan Kita Menulis.
[4]. Manuhutu, M. A., Muttaqin, M., Irmayani, D., Tamara, T., Gustiana, Z., Hazriani, H., ... & Karim, A. (2021). *Pengantar Forensik Teknologi Informasi*. Yayasan Kita Menulis.
[5]. Kizza, J. M., Kizza, W., & Wheeler. (2013). Guide to computer network security.
[6]. Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506.
[7]. Perlman, R., Kaufman, C., & Speciner, M. (2016). Network security: private communication in a public world. Pearson Education India.
[8]. Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. Jurnal Teknoinfo, 12(2), 72-75.
[9]. Wang, J. (2009). Computer network security (pp. 3-24). Berlin/Heidelberg, Germany: Springer.
[10]. Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. J-SIKA|.
[11]. Prasetio, Adhi, Andrew Fernando Pakpahan, Ayudia Popy Sesilia, Bonaraja Purba, Edi Surya Negara, Gilny Aileen Joan Rantung, Ika Yuniwati et al. "Metodologi Penelitian Ilmiah." (2021).
[12]. Simarmata, N. I. P., Hasibuan, A., Rofiki, I., Sukarman, P., Tasnim, T., Sitorus, E., ... & Simarmata, J. (2021). Metode Penelitian Untuk Perguruan Tinggi.