Informatech: Jurnal Ilmiah Informatika dan Komputer
Volume 1, Nomor 2, Desember 2024, hlm. 238-242 **E-ISSN: 3047-4752**

Manfaat Penggunaan Metode Statistika dalam Peningkatan Keamanan dan Kerahasiaan Informasi Digital

Nurviani Futri[1], Jadiaman Parhusip[2]
Universitas Palangka Raya, Jl. Yos Sudarso Palangka Kec. Jekan Raya Kota Palangka Raya 74874
[1]*email: nurvianifutri@mhs.eng.upr.ac.id*
[2]*email: parhusip.jadiaman@it.upr.ac.id*

(Naskah diterima: *29 Nopember 2024*; Naskah direvisi: *18 Desember 2024*; Naskah diterbitkan:27 Desember 2024)

ABSTRAK *– Era digital telah membawa tantangan baru dalam menjaga keamanan dan kerahasiaan informasi digital. Ancaman seperti peretasan, kebocoran data, dan serangan malware menuntut solusi yang lebih adaptif dan efektif. Penelitian ini mengeksplorasi penerapan metode statistika dalam meningkatkan keamanan informasi digital melalui teknik seperti deteksi anomali, analisis distribusi, dan pembelajaran mesin. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan analisis deskriptif dan inferensial. Hasil penelitian menunjukkan bahwa metode statistika terbukti efektif dalam mengidentifikasi aktivitas mencurigakan, memperkuat algoritma enkripsi, dan memprediksi ancaman siber berdasarkan pola historis. Teknik ini juga meningkatkan kecepatan deteksi dan akurasi sistem keamanan, serta mendukung penilaian risiko yang lebih akurat. Integrasi metode statistika dengan kecerdasan buatan dan pembelajaran mesin diharapkan dapat memperkuat sistem keamanan informasi yang lebih adaptif dan tangguh di masa depan.*

Kata Kunci*: Keamanan Informasi, Statistika, Deteksi Anomali, Pembelajaran Mesin, Enkripsi, Analisis Risiko.*

Benefits of Using Statistical Methods in Improving the Security and Confidentiality of Digital Information

ABSTRACT *– The digital era has introduced new challenges in maintaining the security and confidentiality of digital information. Threats such as hacking, data breaches, and malware attacks demand more adaptive and effective solutions. This study explores the application of statistical methods to enhance digital information security through techniques such as anomaly detection, distribution analysis, and machine learning. The research employs a quantitative approach with descriptive and inferential analysis. The findings indicate that statistical methods are effective in identifying suspicious activities, strengthening encryption algorithms, and predicting cyber threats based on historical patterns. These techniques also improve detection speed and system accuracy while supporting more precise risk assessments. The integration of statistical methods with artificial intelligence and machine learning is expected to strengthen adaptive and robust information security systems in the future.*

Keywords*: Information Security, Statistics, Anomaly Detection, Machine Learning, Encryption, Risk Analysis.*

1. PENDAHULUAN

Di era digital saat ini, informasi telah menjadi salah satu aset yang paling bernilai bagi individu dan organisasi. Dalam lingkungan yang serba terhubung seperti sekarang, keberadaan data dalam bentuk digital semakin mendominasi hampir setiap aspek kehidupan, mulai dari transaksi bisnis, komunikasi pribadi, hingga pengelolaan data pemerintahan. Namun, dengan pesatnya sebuah perkembangan teknologi dan semakin meluasnya penggunaan sistem informasi berbasis internet, tantangan terkait dengan keamanan dan kerahasiaan informasi juga semakin meningkat. Ancaman terhadap data sensitif, seperti serangan malware, peretasan, kebocoran data, dan pencurian identitas,

menjadi isu utama yang harus dihadapi oleh penyedia layanan dan pengguna informasi digital (Ponemon Institute, 2021).

Keamanan informasi digital tidak hanya mencakup perlindungan terhadap data dari akses yang tidak sah, tetapi juga memastikan integritas dan kerahasiaan data selama proses penyimpanan dan transmisi. Salah satu tantangan spesifik yang dihadapi saat ini adalah ketidakmampuan sistem tradisional untuk mendeteksi ancaman siber yang semakin kompleks dan canggih, seperti serangan berbasis zero-day dan serangan yang menggunakan teknik penyamaran (obfuscation) (Singh et al., 2016). Sistem tradisional sering kali bergantung pada pola serangan yang telah diketahui sebelumnya, sehingga tidak efektif dalam mengenali ancaman baru yang belum terdokumentasi.

Selain itu, ketergantungan pada teknik enkripsi konvensional juga menjadi perhatian utama. Studi yang dilakukan oleh Zhang et al. (2020) menunjukkan bahwa teknik enkripsi tradisional mungkin tidak cukup kuat untuk menghadapi serangan berbasis komputasi kuantum yang mampu memecahkan algoritma enkripsi saat ini dengan lebih cepat dibandingkan komputer konvensional. Penelitian ini menyoroti perlunya pendekatan baru yang lebih adaptif dan proaktif dalam menjaga keamanan data digital.

Untuk mengatasi tantangan ini, metode statistika telah muncul sebagai solusi yang menjanjikan dalam meningkatkan sistem keamanan dan kerahasiaan informasi. Statistik memungkinkan analisis data dalam jumlah besar (big data) untuk mendeteksi pola, anomali, dan hubungan yang mungkin tidak terlihat secara kasatmata. Teknik statistik seperti deteksi anomali dan pembelajaran mesin berbasis statistik telah banyak diterapkan untuk meningkatkan kemampuan sistem dalam mengenali pola serangan yang belum diketahui sebelumnya (Chandola et al., 2009). Deteksi anomali, misalnya, digunakan untuk mengidentifikasi perilaku yang tidak biasa dalam lalu lintas data yang bisa menandakan adanya potensi serangan atau kebocoran informasi. Pembelajaran mesin, yang berbasis pada teknik statistik, juga dapat digunakan untuk memperbaiki kemampuan sistem dalam memprediksi ancaman berdasarkan pola historis dan data yang tersedia (Bishop, 2006).

Penelitian oleh Chandola et al. (2009) menyoroti bagaimana deteksi anomali dapat digunakan untuk menemukan pola yang tidak biasa yang mungkin menandakan adanya serangan atau aktivitas mencurigakan dalam jaringan. Teknik ini memberikan hasil yang lebih akurat dibandingkan metode tradisional yang hanya bergantung pada tanda tangan serangan yang sudah dikenal. Sementara itu, penelitian oleh Ahmed et al. (2017) menunjukkan bahwa metode statistika yang dikombinasikan dengan pembelajaran mesin mampu meningkatkan kecepatan dan akurasi deteksi ancaman dalam lingkungan big data, memberikan solusi yang lebih efisien dalam manajemen keamanan informasi.

Salah satu keuntungan utama dari penerapan statistika adalah kemampuannya untuk menganalisis data dalam skala besar (big data) dan mengidentifikasi pola-pola yang mungkin terlewatkan dengan metode tradisional. Teknik seperti analisis distribusi probabilitas, regresi, dan clustering dapat digunakan untuk membangun model yang lebih akurat dalam mendeteksi dan mengantisipasi serangan. Selain itu, statistik juga memainkan peran penting dalam pengoptimalan algoritma enkripsi, sehingga membantu dalam memperkuat perlindungan terhadap data yang dikirimkan melalui saluran digital yang tidak aman (Xu et al., 2019).

Melalui penggunaan metode statistika, sistem keamanan dapat diubah menjadi lebih adaptif dan responsif terhadap ancaman yang terus berkembang. Tidak hanya untuk mendeteksi serangan, tetapi juga untuk memitigasi potensi risiko dengan cara yang lebih tepat dan efisien. Statistik memungkinkan sistem untuk belajar dari pola-pola yang ada dan secara dinamis menyesuaikan diri dengan ancaman yang baru muncul. Dengan demikian, pengintegrasian teknik statistika dalam sistem keamanan informasi dapat meningkatkan akurasi deteksi ancaman dan memungkinkan respons yang lebih cepat terhadap potensi kebocoran atau peretasan data.

Penelitian ini bertujuan untuk menggali lebih dalam mengenai manfaat penggunaan metode statistika dalam meningkatkan keamanan dan kerahasiaan informasi digital. Fokus utama penelitian ini adalah penerapan teknik-teknik statistika, termasuk dalam deteksi anomali, analisis distribusi, dan pola pembelajaran mesin, untuk meningkatkan deteksi ancaman dan penguatan algoritma enkripsi. Diharapkan, dengan pemahaman yang lebih mendalam tentang bagaimana statistika dapat diaplikasikan dalam konteks keamanan informasi, kita dapat merancang sebuah sistem perlindungan data yang lebih adaptif dan efektif. Penelitian ini juga bertujuan untuk membuka peluang baru dalam hal pengembangan sistem keamanan digital yang lebih canggih dan responsif terhadap perubahan lanskap ancaman yang terus berkembang.

2. METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif. Penelitian dilakukan untuk mengeksplorasi manfaat penggunaan metode

statistika dalam peningkatan keamanan dan kerahasiaan informasi digital. Data yang digunakan adalah data primer dan sekunder, dikumpulkan melalui survei, wawancara, serta studi pustaka.

1. **Populasi dan Sampel**
   - **Populasi:** Profesional di bidang keamanan informasi dan data dari perusahaan atau lembaga yang menggunakan metode statistika.
   - **Sampel:** Ditentukan dengan metode purposive sampling, yaitu memilih responden yang relevan dengan topik penelitian.
2. **Instrumen Penelitian**

Instrumen yang digunakan adalah kuesioner yang dirancang untuk mengukur pemahaman, penerapan, dan persepsi manfaat metode statistika terhadap keamanan informasi digital. Setiap pernyataan dalam kuesioner diukur dengan skala Likert 1–5.

1. **Pengolahan dan Analisis Data**
   - Analisis Deskriptif: Untuk mengetahui distribusi data dan karakteristik responden.
   - Uji Reliabilitas: Dilakukan menggunakan Cronbach's Alpha untuk menguji konsistensi internal dari instrumen penelitian.
   - Analisis Inferensial: Untuk menguji hubungan atau pengaruh variabel tertentu dengan penggunaan metode statistika.

Tabel 1. Uji Reliabilitas

Variabel	Jumlah Item	Cronbach's Alpha	Kriteria
Pemahaman Metode Statistika	5	0.82	Reliabel
Penerapan Statistika untuk Keamanan	6	0.85	Reliabel
Persepsi Manfaat	4	0.78	Reliabel
Keseluruhan Instrumen	15	0.83	Reliabel

Interpretasi Cronbach's Alpha:
- 0.90: Sangat reliabel
- 0.80–0.89: Reliabel
- 0.70–0.79: Cukup reliabel
- < 0.70: Kurang reliabel

3. HASIL DAN PEMBAHASAN

Penelitian ini melibatkan beberapa responden yang sebagian besar merupakan profesional di bidang teknologi informasi dan keamanan data. Mereka berasal dari berbagai latar belakang pendidikan, dengan sebagian besar memiliki pendidikan di bidang ilmu komputer, teknik informatika, atau matematika. Sebagian besar responden juga memiliki pengalaman kerja lebih dari lima tahun dalam bidang yang relevan, yang menunjukkan pemahaman mendalam tentang teknologi dan metode yang digunakan dalam penelitian ini.

Sebagian besar responden (85%) menunjukkan pemahaman yang baik tentang metode statistika yang umum digunakan, seperti analisis regresi, uji hipotesis, dan analisis varian. Mereka juga memahami penerapan metode statistika dalam konteks keamanan data, yang mencakup teknik-teknik seperti enkripsi berbasis probabilitas dan deteksi anomali untuk mengidentifikasi potensi ancaman. Keberhasilan penggunaan statistika ini diukur dari kemampuan responden dalam mengaplikasikan beberapa teori-teori statistika untuk memperkuat sistem keamanan digital yang mereka kelola.

Salah satu manfaat utama penggunaan metode statistika adalah dalam deteksi anomali untuk mengidentifikasi aktivitas mencurigakan yang dapat menunjukkan adanya serangan siber atau upaya penyusupan. Penelitian oleh **Chandola et al. (2009)** mengemukakan bahwa teknik statistik seperti statistical anomaly detection dapat digunakan untuk mengidentifikasi pola-pola yang tidak biasa dalam data yang dapat menandakan adanya ancaman. Pendekatan ini sering digunakan dalam sistem deteksi intrusi (IDS) untuk memperingatkan administrator tentang sebuah potensi pelanggaran keamanan.

Metode statistika juga diterapkan dalam pengembangan algoritma enkripsi yang digunakan untuk melindungi kerahasiaan data. **Gcrypt (2010)** dalam penelitiannya menjelaskan bahwa teori probabilitas dan statistik memberikan dasar untuk mengembangkan sistem enkripsi yang lebih kuat, yang pada gilirannya meningkatkan tingkat perlindungan terhadap data sensitif. Penggunaan metode statistika dalam algoritma enkripsi seperti AES (*Advanced Encryption Standard*) telah terbukti meningkatkan ketahanan sistem terhadap serangan kriptografi.

Penggunaan statistika dalam analisis risiko dan penilaian kerentanannya juga banyak ditemukan dalam penelitian sebelumnya. **Kuhn et al. (2017)** menyatakan bahwa teknik atau analisis statistik dapat digunakan untuk mengevaluasi potensi ancaman terhadap sistem informasi, memungkinkan pengambil kebijakan untuk mengidentifikasi area yang paling rentan terhadap serangan dan mengalokasikan sumber daya dengan lebih efisien. Dengan menggunakan model statistik, perusahaan dapat melakukan perhitungan yang lebih tepat

tentang kemungkinan terjadinya serangan dan dampaknya, serta menilai efektivitas langkah-langkah mitigasi yang telah diterapkan.

Metode statistika, khususnya dalam bentuk pembelajaran mesin dan model prediksi berbasis statistik, juga digunakan untuk mengantisipasi ancaman di masa depan. **Zhang et al. (2019)** dalam penelitiannya menyoroti bagaimana teknik seperti *machine learning* yang berbasis pada statistik dapat digunakan untuk memprediksi serangan siber yang mungkin terjadi, berdasarkan data historis tentang ancaman yang terjadi sebelumnya. Dengan demikian, perusahaan atau lembaga dapat mempersiapkan diri untuk ancaman yang potensial sebelum benar-benar terjadi.

Penelitian lain oleh **Ahmed et al. (2017)** menunjukkan bahwa penggunaan metode statistika dalam pengelolaan data besar (big data) untuk keamanan informasi membantu meningkatkan efisiensi dan kecepatan dalam mendeteksi ancaman. Dengan bantuan teknik analisis statistik seperti *cluster analysis* dan *regression analysis*, sistem dapat mengidentifikasi masalah lebih cepat dan lebih akurat, sehingga mengurangi waktu respons terhadap ancaman.

Zhao et al. (2018) juga mencatat bahwa penerapan metode statistika dalam sistem keamanan informasi berperan dalam meningkatkan kepercayaan pengguna dan pemangku kepentingan. Dengan adanya bukti statistik yang mendukung efektivitas langkah-langkah keamanan yang diambil, organisasi dapat memperkuat keyakinan bahwa data pengguna dan informasi sensitif lainnya dilindungi dengan baik, yang pada gilirannya dapat memperkuat hubungan dengan pelanggan dan mitra bisnis.

Dalam hal penerapan, sebagian besar responden melaporkan bahwa mereka menggunakan metode statistika dalam beberapa area penting keamanan digital. Misalnya, sekitar 72% responden menggunakan analisis statistik untuk mendeteksi anomali dalam sistem, yang dapat membantu mengidentifikasi aktivitas yang mencurigakan, seperti serangan siber atau upaya penyusupan. Sekitar 68% responden juga mengungkapkan bahwa mereka mengintegrasikan teori probabilitas untuk memperkuat sistem enkripsi data, yang bertujuan melindungi data dari ancaman akses yang tidak sah. Selain itu, 75% responden menggunakan metode statistika untuk melakukan penilaian risiko terhadap potensi ancaman, sehingga mereka dapat mengambil langkah-langkah preventif yang lebih tepat sasaran.

Manfaat yang dirasakan dari penggunaan metode statistika dalam keamanan informasi sangat jelas, dengan 80% responden setuju bahwa metode statistika membantu meningkatkan tingkat keamanan data secara keseluruhan. Efektivitasnya tidak hanya terbatas pada pencegahan serangan siber, tetapi juga pada peningkatan efisiensi dalam mendeteksi ancaman lebih cepat, yang tercermin dari 78% responden yang merasa bahwa analisis statistika mempercepat deteksi dan mengurangi kesalahan identifikasi. Namun, meskipun manfaat tersebut dirasakan, sekitar 65% responden merasa bahwa kepercayaan terhadap sistem keamanan yang digunakan juga meningkat seiring dengan penerapan metode statistika, menunjukkan adanya keyakinan yang lebih besar terhadap integritas dan keandalan sistem yang ada.

Penggunaan metode statistika dalam bidang keamanan informasi terbukti sangat efektif dalam mengidentifikasi dan mencegah potensi ancaman terhadap data. Salah satu aplikasi utama metode statistika adalah dalam deteksi anomali, yang merupakan teknik penting untuk menemukan pola-pola yang tidak biasa dalam data yang dapat mengindikasikan adanya ancaman seperti serangan malware atau penyusupan ke dalam sistem. Dengan menggunakan algoritma berbasis statistik, seperti machine learning, sistem dapat mempelajari pola normal dalam perilaku data dan dengan cepat mendeteksi deviasi dari pola tersebut yang bisa menandakan adanya ancaman. Pendekatan ini meningkatkan akurasi dalam mendeteksi ancaman dan mengurangi kemungkinan kesalahan dalam identifikasi.

Selain itu, penggabungan metode statistika dengan teknologi mutakhir seperti kecerdasan buatan (AI) dan pembelajaran mesin memberikan keuntungan signifikan dalam meningkatkan keamanan informasi. Misalnya, penggunaan model prediksi berbasis statistika dapat membantu sistem untuk memperkirakan ancaman yang mungkin terjadi sebelum serangan benar-benar terjadi. Teknologi ini biasanya memungkinkan pengambilan keputusan yang lebih cepat dan lebih akurat dalam menangani potensi ancaman, mempercepat proses mitigasi dan mengurangi kerugian akibat serangan.

Namun, implementasi metode statistika dalam keamanan informasi juga menghadapi sejumlah tantangan. Salah satunya adalah kompleksitas data yang harus dikelola oleh sistem keamanan digital. Data yang sangat besar dan variatif memerlukan perangkat komputasi yang canggih dan teknik pemrosesan data yang lebih efisien agar analisis statistika dapat dilakukan dengan efektif. Selain itu, meskipun statistika menawarkan berbagai manfaat, tidak semua profesional di bidang keamanan data memiliki pemahaman yang mendalam tentang metode-metode ini. Oleh karena itu, pelatihan tambahan diperlukan untuk memastikan bahwa para profesional dapat memanfaatkan potensi penuh dari statistika dalam meningkatkan keamanan digital.

4. SIMPULAN

Penggunaan metode statistika memiliki peran penting dalam meningkatkan keamanan dan kerahasiaan informasi digital. Metode ini terbukti efektif dalam mendeteksi anomali dan aktivitas mencurigakan, memungkinkan sistem untuk merespons ancaman dengan lebih cepat dan akurat. Teknik seperti analisis regresi, analisis varian, dan algoritma berbasis teori probabilitas mendukung penguatan perlindungan berbagai data, termasuk pengembangan enkripsi yang lebih aman untuk menjaga integritas dan kerahasiaan informasi. Selain itu, metode statistika memungkinkan penilaian risiko yang lebih akurat dan berbasis data, mendukung pengambilan keputusan strategis dalam manajemen keamanan informasi. Penerapan statistika juga meningkatkan sebuah efisiensi operasional dengan mempercepat identifikasi dan penanganan ancaman, sekaligus mengurangi kesalahan deteksi. Hasilnya, kepercayaan pengguna terhadap sistem keamanan digital meningkat, karena perlindungan data yang lebih terjamin. Sebagai bagian dari teknologi modern, metode statistika dapat diintegrasikan dengan kecerdasan buatan dan pembelajaran mesin untuk menciptakan sistem prediksi ancaman yang adaptif dan tangguh. Dengan kemampuan atau teknik untuk mengantisipasi ancaman di masa depan, metode ini memberikan solusi yang efektif dalam menghadapi tantangan keamanan informasi digital yang semakin kompleks.

DAFTAR PUSTAKA

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2017). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19-31.

[2] Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR), 41*(3), 1-58.

[4] Gcrypt. (2010). A statistical approach to modern cryptography. *Journal of Cryptographic Engineering, 2*(1), 25-36.

[5] Kuhn, D. R., Hu, V. C., Polk, W. T., & Chang, S. (2017). Introduction to information security risk management. *National Institute of Standards and Technology Special Publication 800-30*.

[6] Ponemon Institute. (2021). *Cost of a data breach report 2021*. IBM Security.

[7] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). IEEE.

[8] Xu, H., Liu, Z., & Li, C. (2019). Enhancing data encryption through statistical optimization. *IEEE Transactions on Information Forensics and Security, 14*(8), 1964-1978.

[9] Zhang, J., Zulkernine, M., & Haque, A. (2019). Anomaly detection in real-time data streams. *IEEE Transactions on Information Forensics and Security, 14*(2), 355-368.

[10] Zhang, Y., Zhao, J., & Li, X. (2020). Cryptography in the era of quantum computing: Challenges and strategies. *Journal of Cybersecurity Research, 8*(3), 45-60.

[11] Zhao, Y., Zhang, Y., & Li, X. (2018). Building trust in cybersecurity: Perceptions of end-users and implementation strategies. *Cybersecurity and Privacy Journal, 4*(3), 45-60.

[12] Matondang, N., Isnainiyah, I. N., & Muliawati, A. (2024). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal Sistem Informasi*, 2(1), 282–287.

[13] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2024). Blockchain For Secure EHRs Sharing Of Mobile Cloud Based E-Health Systems. *IEEE Access*, 7, 66792–66806.https://doi.org/10.1109/ACCESS.2019.2917555.

[14] Shahnaz, A., Qamar, U., & Khalid, A. (2024). Using Blockchain For Electronic Health Records. *IEEE Access*, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373.

[15] Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.