Peran Sistem Pencegahan Intrusi dalam Memperkuat Keamanan Siber Indonesia Terhadap Eksploitasi Kriptografi Dasar.

Oleh:

Benony Gabriel (NIM: 105222002)

Ridho Pratama Widiantoro (NIM: 105222011)

Pendahuluan

Di era digital yang semakin berkembang pesat, keamanan siber menjadi salah satu pilar utama dalam menjaga stabilitas informasi dan keberlangsungan sistem digital di berbagai sektor, baik pemerintahan, pendidikan, maupun industri. Digitalisasi yang masif telah membawa berbagai kemudahan dalam kehidupan manusia, namun di sisi lain juga menghadirkan potensi risiko yang sangat besar jika tidak dibarengi dengan sistem pengamanan yang memadai. Salah satu komponen penting dalam infrastruktur keamanan informasi adalah kriptografi, yaitu teknik yang digunakan untuk melindungi informasi dengan cara mengubah data menjadi bentuk yang tidak dapat dipahami tanpa kunci khusus. Kriptografi telah lama digunakan untuk menjaga kerahasiaan, integritas, dan keaslian data, terutama dalam komunikasi digital dan transaksi daring.

Namun, seiring dengan meningkatnya kemampuan komputasi dan kecanggihan teknik serangan siber, berbagai algoritma kriptografi dasar yang dulunya dianggap aman kini mulai terancam. Beberapa algoritma kriptografi lama seperti RSA (Rivest–Shamir–Adleman) dengan panjang kunci rendah, SHA-1 (*Secure Hash Algorithm*), dan protokol enkripsi yang tidak lagi direkomendasikan telah terbukti memiliki celah keamanan yang dapat dieksploitasi oleh penyerang dengan teknik modern [1][2]. Hal ini menjadi sangat berbahaya mengingat masih banyak sistem informasi di Indonesia yang menggunakan protokol atau algoritma kriptografi yang rentan akibat minimnya pembaruan sistem atau kurangnya pemahaman teknis.

Eksploitasi terhadap kelemahan kriptografi bukanlah ancaman teoritis semata, melainkan telah terjadi dalam berbagai bentuk serangan nyata. Salah satu contohnya adalah serangan *man-in-the-middle* (MITM) yang memanfaatkan kerentanan pada protokol TLS versi lama atau penggunaan sertifikat digital yang lemah [3]. Selain itu, serangan *brute-force* terhadap sistem autentikasi berbasis hash dan serangan *ransomware* yang mengenkripsi file korban juga kerap memanfaatkan kelemahan dalam penerapan kriptografi [4]. Beberapa serangan bahkan menggunakan koneksi terenkripsi sebagai medium untuk menyembunyikan aktivitas berbahaya dari sistem keamanan yang konvensional, sehingga ancaman tidak terdeteksi hingga terlambat.

Dalam konteks ini, kehadiran Sistem Pencegahan Intrusi atau *Intrusion Prevention System* (IPS) menjadi sangat relevan. IPS merupakan sistem keamanan jaringan yang mampu mendeteksi dan secara proaktif menghentikan aktivitas berbahaya dalam jaringan secara real-time [5]. Tidak seperti sistem deteksi intrusi (IDS) yang hanya memberi peringatan, IPS juga memiliki kemampuan untuk mengambil tindakan otomatis seperti memblokir lalu lintas mencurigakan atau memutus koneksi dengan sumber ancaman [5]. IPS dapat mendeteksi

berbagai serangan yang ditujukan untuk mengeksploitasi kelemahan dalam implementasi kriptografi, baik itu dengan mendeteksi anomali pada pola lalu lintas jaringan, payload mencurigakan, hingga upaya komunikasi dengan server yang menggunakan algoritma kriptografi lemah.

Sayangnya, meskipun potensi ancaman sangat nyata, implementasi IPS di Indonesia masih tergolong terbatas. Banyak institusi, terutama di sektor pemerintahan dan pendidikan, belum memiliki sistem keamanan yang memadai karena keterbatasan anggaran, sumber daya manusia, dan kurangnya kesadaran akan pentingnya perlindungan terhadap serangan yang semakin canggih. Selain itu, teknologi IPS membutuhkan pemeliharaan dan pembaruan yang berkelanjutan agar mampu mengikuti perkembangan jenis serangan baru, termasuk serangan yang menyasar kriptografi.

Berdasarkan latar belakang tersebut, tulisan ini mencoba merumuskan dua pertanyaan utama yang akan dijawab melalui pembahasan dalam esai ini: (1) Bagaimana sistem pencegahan intrusi (IPS) dapat membantu mendeteksi dan mencegah eksploitasi terhadap kelemahan kriptografi? dan (2) Apa saja tantangan yang dihadapi dalam penerapan IPS di Indonesia, baik dari segi teknis, kebijakan, maupun sumber daya?

Adapun tujuan dari penulisan esai ini adalah untuk menjelaskan secara komprehensif peran IPS dalam melindungi sistem informasi dari eksploitasi terhadap kriptografi yang lemah, serta mengkaji tantangan dan hambatan yang dihadapi dalam implementasi IPS di Indonesia. Dengan demikian, diharapkan tulisan ini dapat memberikan kontribusi terhadap pemahaman yang lebih mendalam mengenai pentingnya strategi pertahanan proaktif dalam menghadapi ancaman keamanan siber, serta memberikan rekomendasi kebijakan dan solusi teknis yang relevan guna memperkuat ketahanan siber nasional.

Pembahasan

Kriptografi merupakan cabang ilmu yang berfokus pada pengamanan informasi dengan mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu. Secara umum, kriptografi mencakup tiga fungsi utama: enkripsi, yaitu proses mengubah pesan asli menjadi bentuk terenkripsi; dekripsi, yaitu proses mengembalikan pesan terenkripsi menjadi bentuk aslinya; serta autentikasi, yang memastikan keaslian dan integritas pesan [6].

Algoritma kriptografi terbagi menjadi dua jenis utama, yaitu algoritma simetris dan asimetris [6]. Algoritma simetris seperti Advanced Encryption Standard (AES) menggunakan kunci yang sama untuk enkripsi dan dekripsi, sementara algoritma asimetris seperti Rivest–Shamir–Adleman (RSA) menggunakan pasangan kunci publik dan privat. Selain itu, terdapat fungsi hash kriptografis seperti SHA-1 dan SHA-256 yang digunakan untuk verifikasi integritas data [7]. Meskipun algoritma kriptografi modern dirancang untuk tahan terhadap serangan, implementasi yang keliru atau konfigurasi yang lemah dapat menimbulkan celah keamanan serius. Salah satu masalah umum adalah penggunaan panjang kunci yang terlalu pendek, seperti RSA dengan kunci 1024-bit yang kini sudah tidak direkomendasikan karena rentan terhadap serangan faktorisasi [8]. Selain itu, penggunaan kembali nonce dalam algoritma seperti AES-GCM dapat menyebabkan kebocoran informasi dan membuka kemungkinan serangan *plaintext recovery.*

Penggunaan kunci statis yang tidak dirotasi secara berkala juga menjadi masalah besar dalam sistem yang bergantung pada kerahasiaan kunci. Tidak hanya itu, beberapa sistem masih menggunakan algoritma yang telah dinyatakan tidak aman, seperti SHA-1, yang sejak 2017 telah dibuktikan dapat dipalsukan melalui serangan *collision* [9]. Celah-celah ini seringkali muncul bukan karena kelemahan algoritmanya sendiri, melainkan karena kurangnya pemahaman pengembang dalam praktik kriptografi yang benar.

Eksploitasi terhadap sistem kriptografi dapat dilakukan melalui berbagai jenis serangan. Serangan *brute-force* adalah metode paling dasar yang mencoba semua kemungkinan kunci hingga menemukan yang benar, dan sangat efektif terhadap sistem dengan kunci pendek. *Cryptanalysis* atau analisis kripto merupakan teknik yang memanfaatkan kelemahan matematis dalam algoritma untuk memecahkan enkripsi tanpa mengetahui kunci rahasia. Salah satu ancaman paling berbahaya adalah serangan *man-in-the-middle (MITM)*, di mana penyerang menyisipkan dirinya di antara dua pihak yang berkomunikasi dan dapat membaca atau memodifikasi pesan yang dikirim tanpa terdeteksi. MITM sering berhasil ketika protokol enkripsi tidak memverifikasi sertifikat dengan benar atau menggunakan kunci publik yang tidak divalidasi [10].

Selain itu, terdapat serangan yang mengeksploitasi kelemahan pada implementasi fisik kriptografi, yang dikenal sebagai *side-channel attacks*. Serangan ini tidak menyerang algoritma secara langsung, melainkan menganalisis informasi bocor seperti waktu proses, konsumsi daya, atau radiasi elektromagnetik untuk memperoleh kunci rahasia. Penelitian oleh Kocher et al. menunjukkan bahwa variasi waktu dalam operasi RSA dapat dimanfaatkan untuk memulihkan kunci privat [11]. Ancaman-ancaman ini menegaskan bahwa sistem kriptografi tidak hanya harus dirancang secara matematis kuat, tetapi juga diimplementasikan dengan cermat dan dilengkapi perlindungan terhadap serangan fisik dan jaringan.

Sistem Pencegahan Intrusi (*Intrusion Prevention System/IPS*) adalah komponen penting dalam keamanan jaringan yang dirancang untuk tidak hanya mendeteksi aktivitas mencurigakan atau berbahaya, tetapi juga menghentikan aktivitas tersebut sebelum menimbulkan kerusakan lebih lanjut. Dalam konteks keamanan jaringan, IPS sering kali dibandingkan dengan sistem deteksi intrusi (*Intrusion Detection System/IDS*). Perbedaan mendasar antara keduanya terletak pada sifat responsnya: IDS bersifat pasif, yakni hanya memberikan notifikasi atau laporan kepada administrator saat terdeteksi ancaman, sementara IPS bersifat aktif, yaitu mampu mengambil tindakan otomatis seperti memblokir lalu lintas atau menghentikan sesi yang mencurigakan [5]. Fungsi utama dari IPS adalah untuk melindungi sistem dari eksploitasi kerentanan, baik itu yang berasal dari luar jaringan maupun dari dalam. IPS bekerja dengan cara menyaring lalu lintas jaringan dan menganalisis pola-pola data untuk mendeteksi adanya aktivitas yang mencurigakan atau sesuai dengan tanda-tanda serangan yang telah dikenal sebelumnya. Ketika potensi ancaman terdeteksi, sistem ini akan segera mengambil tindakan untuk mencegah masuknya ancaman tersebut ke dalam jaringan atau sistem target [5].

Teknologi *IDPS (Intrusion Detection and Prevention System)* menggunakan berbagai metode untuk mendeteksi insiden. Tiga kelas utama dari metode deteksi yang perlu dibahas adalah metode berbasis tanda tangan (*signature-based*), berbasis anomali (*anomaly-based*), dan analisis protokol berkeadaan (*stateful protocol analysis*) [12]. Ketiganya memiliki

keunggulan dan kelemahan masing-masing, sehingga banyak teknologi IDPS menggabungkan lebih dari satu metode untuk menghasilkan deteksi yang lebih komprehensif dan akurat [12].

Metode deteksi berbasis tanda tangan (*signature-based detection*) bekerja dengan cara mencocokkan pola atau karakteristik ancaman yang sudah diketahui sebelumnya dengan kejadian yang sedang terjadi. Jika pola yang sama terdeteksi, maka sistem dapat memberikan peringatan. Namun, pendekatan ini cenderung hanya efektif dalam mendeteksi ancaman yang sudah dikenal dan mungkin kurang responsif terhadap ancaman baru atau serangan dengan pola yang sedikit berbeda dari yang telah terdokumentasi [12].

Di sisi lain, deteksi berbasis anomali (*anomaly-based detection*) beroperasi dengan membandingkan aktivitas yang terjadi dengan definisi atau profil aktivitas yang dianggap normal. Aktivitas yang menyimpang dari pola normal ini akan dianggap sebagai anomali atau potensi ancaman. Metode ini berguna dalam mengidentifikasi ancaman yang sebelumnya tidak dikenal, namun memiliki risiko tinggi dalam menghasilkan peringatan palsu (*false positives*), karena penyimpangan kecil dalam aktivitas normal juga dapat terdeteksi sebagai ancaman [12].

Sementara itu, analisis protokol berkeadaan (*stateful protocol analysis*) memperhatikan status atau kondisi protokol tertentu dan membandingkannya dengan standar yang telah ditetapkan. Tujuannya adalah untuk mengidentifikasi penyimpangan dalam cara protokol digunakan. Metode ini memanfaatkan profil universal yang dikembangkan oleh penyedia teknologi untuk mengevaluasi bagaimana sebuah protokol seharusnya digunakan dengan aman. Walaupun metode ini dapat mendeteksi berbagai jenis ancaman yang mungkin tidak dikenali oleh metode lain, pengembangan model protokol yang akurat dapat menjadi tantangan besar dan memerlukan sumber daya komputasi yang signifikan [12]. Oleh karena itu, kebanyakan sistem IDPS modern cenderung mengintegrasikan beberapa metode deteksi ini secara bersamaan. Pendekatan integratif semacam ini bertujuan untuk meningkatkan cakupan deteksi dengan menggabungkan keunggulan dari setiap metode, sekaligus meminimalkan kelemahan yang dimiliki masing-masing pendekatan. Dengan demikian, deteksi yang dihasilkan dapat lebih andal dan mampu menghadapi spektrum ancaman keamanan yang lebih luas.

IPS bekerja dengan cara memantau lalu lintas jaringan secara real-time, menganalisis setiap paket data yang masuk maupun keluar dari jaringan. Proses ini dilakukan di titik strategis jaringan, seperti antara router dan switch, atau pada gateway utama menuju internet. IPS dapat mengenali pola-pola tertentu dalam lalu lintas, termasuk upaya pemindaian port, injeksi kode, dan eksploitasi terhadap protokol atau enkripsi. Ketika suatu ancaman terdeteksi, IPS akan secara otomatis mengambil tindakan, seperti memblokir koneksi, mengirimkan peringatan, atau mencatat aktivitas tersebut dalam log untuk keperluan audit dan forensik. Kemampuan respon otomatis ini menjadi keunggulan utama IPS dibandingkan sistem deteksi lainnya. Selain itu, IPS sering kali diintegrasikan dengan sistem keamanan lainnya seperti firewall dan *Security Information and Event Management (SIEM)*. Integrasi ini memungkinkan pengumpulan data ancaman secara terpusat dan pembuatan laporan yang menyeluruh, serta penerapan kebijakan keamanan yang lebih adaptif terhadap ancaman baru [13].

Dengan semakin kompleksnya serangan siber, IPS kini juga mulai mengadopsi teknologi pembelajaran mesin dan kecerdasan buatan untuk meningkatkan kemampuan deteksi dan mengurangi ketergantungan pada tanda tangan manual. Teknologi ini menjadi penting

dalam menghadapi ancaman zero-day dan serangan polymorphic yang sulit dikenali oleh sistem tradisional.

Di era modern, banyak komunikasi data berlangsung melalui saluran terenkripsi seperti HTTPS yang menggunakan protokol SSL/TLS. Namun, meskipun protokol ini dirancang untuk keamanan, mereka tetap rentan terhadap eksploitasi, khususnya jika konfigurasi yang digunakan lemah atau sudah usang. IPS (*Intrusion Prevention System*) memiliki kemampuan untuk mendeteksi serangan terhadap protokol terenkripsi, bahkan ketika payload-nya tidak dapat dilihat secara langsung karena enkripsi. Hal ini dimungkinkan melalui analisis metadata, anomaly detection, dan pemantauan perilaku komunikasi. Salah satu contoh implementasi adalah kemampuan IPS dalam mendeteksi upaya *downgrade attack* terhadap protokol TLS, seperti dalam kasus serangan POODLE yang mengeksploitasi fallback ke SSL 3.0 [14]. Selain itu, IPS juga mampu mengidentifikasi manipulasi paket atau lalu lintas abnormal dalam sesi TLS/HTTPS yang dapat menunjukkan aktivitas *man-in-the-middle* (*MitM*) atau *injection attack*.

Dengan metode inspeksi seperti *Deep Packet Inspection* (*DPI*) dan SSL/TLS fingerprinting, IPS dapat menandai lalu lintas dari sumber yang mencurigakan atau pola komunikasi yang menyimpang dari *baseline* normal, meskipun data terenkripsi. Beberapa vendor bahkan telah mengembangkan modul yang secara khusus dapat mengenali pola serangan seperti *Heartbleed* dalam TLS versi lama.

IPS berperan penting dalam mencegah penggunaan dan akses terhadap sistem yang mengimplementasikan algoritma kriptografi lemah. Misalnya, algoritma seperti RC4, DES, dan bahkan RSA dengan panjang kunci rendah (1024-bit ke bawah) masih ditemukan dalam beberapa sistem lama. IPS dapat dikonfigurasi untuk menolak koneksi yang menggunakan *cipher suite* yang dianggap rentan, baik dari sisi klien maupun server. Dalam lingkungan enterprise, IPS dapat bertindak sebagai filter lalu lintas yang hanya mengizinkan koneksi terenkripsi yang memenuhi standar keamanan tertentu, seperti minimal TLS 1.2 dan cipher modern seperti AES-GCM. Hal ini penting untuk mencegah eksploitasi terhadap cipher lemah seperti RC4 atau protokol yang telah *deprecated*, seperti SSL 2.0 dan SSL 3.0. Selain itu, IPS juga dapat memantau penggunaan sertifikat digital yang tidak valid, seperti yang telah kedaluwarsa, ditandatangani oleh CA tidak terpercaya, atau memiliki parameter kriptografi yang lemah. Dengan kemampuan ini, IPS turut memperkuat postur keamanan jaringan dari sisi transport layer dan membantu organisasi dalam mencapai kepatuhan terhadap standar seperti PCI-DSS atau NIST.

IPS secara aktif dapat mencegah berbagai bentuk eksploitasi terhadap kriptografi dengan melakukan blocking otomatis terhadap serangan brute-force atau dictionary attack. Serangan seperti ini biasanya dilakukan terhadap protokol autentikasi berbasis kriptografi, misalnya SSH, SSL-VPN, atau sistem login berbasis HTTPS. IPS mendeteksi pola lalu lintas dengan frekuensi tinggi atau percobaan login berulang, lalu memutuskan koneksi atau memblokir IP sumber secara otomatis. IPS modern juga diintegrasikan dengan sistem endpoint dan VPN untuk melindungi dari upaya dekripsi paksa atau pemaksaan terhadap channel komunikasi terenkripsi. Sebagai contoh, pada VPN berbasis SSL, IPS dapat mendeteksi jika terjadi anomali dalam pertukaran kunci atau modifikasi struktur paket selama proses handshake yang bisa menunjukkan serangan active eavesdropping.

Meskipun ancaman siber di Indonesia terus meningkat, adopsi teknologi keamanan tingkat lanjut seperti *Intrusion Prevention System* (IPS) masih tergolong rendah. Banyak organisasi, baik di sektor publik maupun swasta, masih mengandalkan firewall konvensional tanpa integrasi dengan IPS, sehingga hanya memberikan perlindungan pada level permukaan dan tidak mampu mendeteksi serangan yang lebih kompleks. Selain itu, banyak pelaku usaha kecil dan menengah (UKM) serta lembaga pendidikan belum melihat IPS sebagai prioritas investasi, sering kali karena keterbatasan anggaran dan kurangnya kesadaran terhadap risiko kriptografi dan serangan canggih seperti *Advanced Persistent Threat* (APT) atau exploit terhadap protokol terenkripsi.

Salah satu hambatan utama dalam penerapan IPS di Indonesia adalah keterbatasan tenaga ahli keamanan siber. Konfigurasi dan pengelolaan IPS membutuhkan keahlian teknis yang mendalam, termasuk pemahaman tentang trafik jaringan, *signature-based analysis*, serta deteksi anomali. Kurangnya pelatihan dan pendidikan khusus di bidang *network security* juga menyebabkan banyak sistem IPS yang telah dipasang tidak dikonfigurasi secara optimal, bahkan dibiarkan dalam pengaturan default sehingga rentan terhadap bypass dan false negative. Selain itu, budaya keamanan informasi masih belum terintegrasi secara menyeluruh dalam pengambilan kebijakan teknologi informasi organisasi, khususnya di sektor pemerintahan dan pendidikan.

Tantangan lain yang signifikan adalah ketimpangan infrastruktur TI di berbagai daerah di Indonesia. Banyak institusi, khususnya di wilayah luar Jawa, masih menggunakan jaringan dengan bandwidth rendah dan perangkat keras yang sudah usang, sehingga menyulitkan implementasi sistem IPS yang membutuhkan sumber daya komputasi cukup besar. Ketimpangan ini menunjukkan perlunya intervensi kebijakan nasional yang strategis untuk mendorong adopsi sistem keamanan canggih secara lebih merata, baik melalui subsidi, pelatihan, maupun penguatan kebijakan minimum requirement dalam pengelolaan TI sektor publik

Kesimpulan

Di era digital yang semakin kompleks, kriptografi menjadi fondasi utama dalam menjaga kerahasiaan, integritas, dan otentikasi komunikasi data. Namun demikian, masih banyak implementasi algoritma kriptografi yang rentan terhadap eksploitasi, baik karena penggunaan versi usang seperti RSA dengan panjang kunci pendek maupun praktik konfigurasi yang keliru. Celah-celah ini dimanfaatkan oleh berbagai bentuk serangan siber, seperti brute-force, serangan man-in-the-middle, dan bahkan teknik side-channel attack yang canggih.

Dalam konteks ini, *Intrusion Prevention System* (*IPS*) memainkan peran krusial sebagai garda depan dalam sistem pertahanan jaringan. Berbeda dari IDS yang bersifat pasif, IPS secara aktif memonitor dan merespons ancaman secara *real-time*, memblokir lalu lintas berbahaya sebelum mencapai sistem target. Melalui kombinasi teknik *signature-based*, *anomaly-based*, dan *stateful protocol analysis*, IPS mampu mendeteksi serangan terhadap protokol terenkripsi seperti SSL/TLS, serta mencegah penggunaan cipher dan kunci yang tidak aman. Lebih jauh lagi, IPS juga berperan dalam memitigasi serangan brute-force dan melindungi endpoint dari upaya dekripsi paksa melalui VPN maupun jalur terenkripsi lainnya. Namun, implementasi IPS di Indonesia masih menghadapi berbagai tantangan. Tingkat adopsi teknologi keamanan

tingkat lanjut masih rendah, terutama di sektor pemerintahan dan pendidikan. Kesenjangan SDM yang belum mumpuni serta infrastruktur TI yang tidak merata memperparah kondisi ini. Banyak institusi belum memiliki tenaga ahli yang mampu mengelola IPS secara optimal, dan jaringan mereka belum mendukung kebutuhan sumber daya IPS modern.

Dengan demikian, perlu adanya sinergi antara teknologi, kebijakan, dan pengembangan kapasitas SDM untuk mengoptimalkan peran IPS dalam ekosistem keamanan siber Indonesia. Pemerintah, swasta, dan institusi pendidikan harus mengambil langkah proaktif, baik melalui investasi infrastruktur, penyusunan regulasi minimum keamanan jaringan, maupun peningkatan literasi dan pelatihan teknis di bidang keamanan informasi. Hanya dengan pendekatan menyeluruh ini, Indonesia dapat membangun ketahanan digital yang kuat, mampu menangkal eksploitasi terhadap sistem kriptografi, serta siap menghadapi tantangan keamanan siber di masa depan.

Referensi

[1]. D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, Stanford University, 2020.

[2]. G. Leurent and T. Peyrin, “SHA-1 is a Shambles - First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust” *IACR Cryptology ePrint Archive*, Jul. 26, 2020. https://eprint.iacr.org/2020/014

[3]. M. Vizard, “Digital certificates riddled with security weaknesses - Security Boulevard,” *Security Boulevard*, Aug. 01, 2023. https://securityboulevard.com/2023/08/digital-certificates-riddled-with-security-weaknesses/

[4]. R. P. Sari, “Apa itu Brute Force Attack: Pengertian, Metode & Cara Mencegahnya,” *CyberHub Indonesia*. Aug. 08, 2024. https://cyberhub.id/pengetahuan-dasar/apa-itu-brute-force-attack

[5]. N. Chakraborty, "Intrusion detection system and intrusion prevention system: A comparative study," *International Journal of Computing and Business Research (IJCBR)*, vol. 4, no. 2, pp. 1–8, 2013.

[6]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.

[7]. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[8]. E. Barker and A. Roginsky, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST Special Publication 800-131A Revision 2, National Institute of Standards and Technology, March 2019. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-131Ar2.

[9]. M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, “The first collision for full SHA-1,” in *advances in Cryptology--CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20--24, 2017, Proceedings, Part I*, vol. 37, pp. 570–596, Springer, 2017.

[10]. A. Mallik, “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS,” *Cyberspace Jurnal Pendidikan Teknologi Informasi*, vol. 2, no. 2, p. 109, Jan. 2019, doi: 10.22373/cj.v2i2.3453.

[11]. P. Kocher, J. Jaffe, B. Jun, dan P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, vol. 1, pp. 5–27, 2011. [Online]. Available: https://doi.org/10.1007/s13389-011-0006-y.
[12]. M. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” *NIST Special Publication 800-94*, 2007. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-94/final.
[13]. IBM, “What is SIEM?” 2023. [Online]. Available: https://www.ibm.com/topics/siem
[14]. A. Prodromou, “Examples of TLS/SSL vulnerabilities TLS Security 6: | Acunetix,” *Acunetix*, Mar. 32, 2019. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/