Original Article

e-XXXX-XXXX

Original Article

Analisis Keamanan Akun Pengguna Terhadap Ancaman Password Guessing

Nur Mutiara Qalbiyah[1]✉, Farah Trialitha[2], Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: nurmutiaraqalbiyah.241031067@mahasiswa.ith.ac.id, farahtrialitha@gmail.com, rakhmadi.rahman@ith.ac.id

Abstrak:

Keamanan siber pada era digital ketika ini menghadapi tantangan yg bersifat multidimensional, meliputi aspek sikap insan, kerentanan aplikasi, sampai infrastruktur serangan otomatis yang massif. Jurnal ini menyajikan studi integratif yang menggabungkan temuan asal 5 pilar utama penelitian keamanan isu. fokus kajian mencakup evaluasi psikologis pencerahan keamanan (security awereness) di Generasi Z, mitigasi eksploitasi teknis melalui SQL Injection, pemodelan prediktif kekuatan kata sandi menggunakan Artificial Neural Networks (ANN), manajemen risiko di objek penting nasional, serta system inferensi spam berbasis infrastruktur (NeightboardWatcher). buatan ini memberikan bahwa pertahanan siber yang efektif harus berpindah berasal contoh reaktif yg berpusat di konten menuju contoh agresif yang berpusat pada perilaku infrastruktur dan optimalisasi komputasi. yg akan terjadi penelitian mengusulkan kerangka kerja pertahanan berlapis yg mengintegrasikan efisiensi prosedur pemecahan di sisi klien memakai pengawasan ketat di tingkat basis data serta jaringan.

Keywords: Keamanan siber, Neural Networks, SQL Injection, Security Awareness, NeightborWatcher.

Pendahuluan

Dibalik pesatnya perkembangan teknologi, kemudahan yang didapat pengguna juga diiringi dengan berbagai tantangan keamanan, salah satunya adalah fenomena password guessing. Fenomena ini terjadi ketika pelaku mencoba menebak kata sandi pengguna dengan harapan mendapatkan akses tidak sah. Dalam dunia keamanan siber, terdapat beberapa teknik umum yang digunakan untuk melakukan password guessing, antara lain Brute Force, Dictionary Attack, dan Credential Stuffing.

Brute Force adalah metode di mana pelaku mencoba setiap kemungkinan kombinasi karakter secara sistematis hingga menemukan kata sandi yang tepat. Dictionary Attack menggunakan daftar kata-kata umum atau yang sering dipakai sebagai kata sandi, sedangkan

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

Credential Stuffing memanfaatkan data kredensial yang bocor dari satu layanan untuk mencoba mengakses layanan lain, mengandalkan fakta bahwa banyak pengguna menggunakan kata sandi yang sama di berbagai platform.

Adanya fenomena password guessing ini disebabkan oleh beberapa faktor, salah satunya adalah pola perilaku manusia yang mudah ditebak. Banyak pengguna masih cenderung menggunakan kata sandi yang sederhana, mudah diingat, atau mengandung informasi pribadi yang mudah diketahui, seperti tanggal lahir, nama anggota keluarga, atau pola keyboard yang umum. Dalam dunia kriptografi, panjang kata sandi sering kali lebih penting daripada kompleksitas karakter karena semakin panjang sebuah kata sandi, semakin sulit untuk ditebak, meskipun karakternya sederhana.

Untuk menghindari risiko password guessing, pengguna dapat menerapkan beberapa praktik keamanan penting. Pertama, penggunaan passphrase—kombinasi beberapa kata yang membentuk kalimat atau frasa yang mudah diingat namun sulit ditebak—dapat meningkatkan kekuatan kata sandi secara signifikan. Kedua, memanfaatkan pengelola kata sandi (password manager) memungkinkan pengguna untuk membuat dan menyimpan kata sandi yang kompleks dan unik untuk setiap layanan tanpa harus mengingat semuanya. Ketiga, mengaktifkan autentikasi dua faktor (two-factor authentication atau 2FA) memberikan lapisan keamanan tambahan dengan mengharuskan verifikasi identitas melalui perangkat lain atau kode khusus, sehingga meskipun kata sandi berhasil ditebak, akses tidak langsung diberikan tanpa faktor kedua tersebut.

Dengan menerapkan langkah-langkah tersebut, pengguna dapat secara efektif mengurangi risiko terkena serangan password guessing dan meningkatkan keamanan data serta akun digital mereka. Penting juga bagi organisasi dan penyedia layanan untuk mengedukasi pengguna tentang pentingnya praktik kata sandi yang kuat serta menyediakan mekanisme keamanan tambahan yang mudah diakses dan digunakan.

Tinjauan Pustaka

Perilaku Kata Sandi dan Uji Kegunaan

Teori kesadaran keamanan informasi menegaskan bahwa pengetahuan saja tidak cukup tanpa adanya perubahan perilaku. Dalam konteks otentikasi, perilaku pengguna terkait penggunaan kata sandi sangat dipengaruhi oleh beban kognitif. Pengguna cenderung memilih kata sandi yang mudah diingat meskipun tingkat keamanan kriptografisnya rendah. Untuk mengukur efektivitas alat bantu keamanan, seperti Kaspersky Password Checker, uji kegunaan dilakukan guna menilai seberapa baik alat tersebut memberikan umpan balik yang membantu pengguna dalam membuat kata sandi yang lebih kuat.

Kerentanan Injeksi pada Basis Data (SQL Injection)

SQL Injection (SQLi) adalah salah satu metode serangan keamanan siber yang paling umum dan berdampak besar, terutama terhadap lapisan data dalam aplikasi web. Kerentanan ini muncul ketika aplikasi menerima data dari pengguna—baik melalui formulir input, parameter URL, atau cookie—dan langsung memasukkan data tersebut ke dalam kueri basis data tanpa melakukan pembersihan, validasi, atau penyaringan yang memadai.

Penyerang memanfaatkan celah ini dengan menyisipkan karakter khusus atau perintah SQL, seperti perintah UNION, ke dalam pernyataan SQL asli yang dijalankan oleh aplikasi. Akibatnya, logika kueri yang seharusnya dijalankan menjadi terganggu dan mengikuti instruksi yang diinginkan penyerang, sehingga memungkinkan akses atau manipulasi data yang tidak sah.

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

Jaringan Saraf Tiruan (Neural Network) dalam Keamanan Kriptografi

Pemanfaatan Jaringan Saraf Tiruan (Neural Network) dalam keamanan siber meliputi penggunaan struktur seperti Recurrent Neural Networks (RNN) atau Long Short-Term Memory (LSTM) untuk memodelkan distribusi kemungkinan kata sandi yang digunakan manusia. Berbeda dengan model Markov tradisional, Neural Network mampu menangkap ketergantungan karakter jangka panjang serta pola substitusi kompleks, seperti leetspeak. Selain itu, model ini dapat diringkas agar efisien dan dapat dijalankan pada perangkat dengan keterbatasan sumber daya.

Infrastruktur Spam dan NeighborWatcher

Dalam dunia spam, pelaku sering memanfaatkan "tempat perlindungan spam" yang berasal dari situs bereputasi baik, seperti forum atau wiki, untuk menyisipkan tautan berbahaya. Teori deteksi yang tidak bergantung pada isi pesan berpendapat bahwa meskipun konten spam dapat sangat bervariasi, infrastruktur yang digunakan oleh pelaku—yaitu jaringan situs yang menjadi target—biasanya relatif tetap.

Sistem NeighborWatcher mengadopsi pendekatan analisis graf untuk mendeteksi serangan spam berdasarkan pola kesamaan target infrastruktur. Dengan metode ini, sistem dapat mengenali serangan yang menggunakan infrastruktur serupa meskipun konten pesan berbeda, sehingga meningkatkan efektivitas deteksi spam.

Metode

Metodologi Analisis Perilaku (Kuantiatif dan Uji Kegunaan)

Metodologi ini melibatkan pengumpulan data secara kuantitatif pada populasi mahasiswa Generasi Z dengan beberapa tahapan sebagai berikut:

1. Survei Kesadaran Keamanan Siber

Survei ini dilakukan untuk mengukur pemahaman responden terhadap ancaman siber yang umum, seperti penipuan daring dan malware. Instrumen survei berupa kuesioner tertutup dengan skala evaluasi, yang bertujuan mengidentifikasi tingkat pengenalan jenis serangan, pemahaman cara kerja ancaman, dan kesadaran akan langkah pencegahan dasar. Hasil survei memberikan gambaran awal mengenai literasi keamanan siber dalam kelompok yang diteliti.

2. Uji Kegunaan Pembuatan Kata Sandi

Peserta diminta membuat kata sandi sesuai kebiasaan mereka tanpa arahan khusus. Kata sandi yang dihasilkan kemudian diuji menggunakan Kaspersky Password Checker untuk mengevaluasi kekuatan berdasarkan kompleksitas, panjang, dan kerentanannya terhadap serangan brute force. Metode ini bertujuan mengamati perilaku nyata pengguna dalam praktik keamanan kata sandi, tidak hanya dari aspek pengetahuan teori.

3. Analisis Deskriptif dan Korelasi Variabel

Data hasil survei dan pengujian kata sandi dianalisis secara deskriptif untuk mengidentifikasi pola dan kecenderungan. Analisis juga mengaitkan variabel latar belakang pendidikan (IT dan Non-IT) serta jenis kelamin dengan kekuatan kata sandi yang dihasilkan.

Metodologi Eksploitasi Teknis (Penetration Testing)

Metode ini fokus pada eksplorasi celah keamanan pada web server, khususnya kerentanan SQL Injection, dengan tahapan sebagai berikut:

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

1. Pengumpulan Informasi (Information Gathering)

Tahapan ini bertujuan mengumpulkan data awal terkait server web dan aplikasi yang diuji. Analisis meliputi struktur URL, parameter yang digunakan, serta teknologi pendukung seperti jenis web server, bahasa pemrograman, dan sistem basis data. Informasi ini menjadi dasar untuk mengidentifikasi titik akses potensial bagi serangan SQL Injection.

2. Deteksi Kerentanan (Vulnerability Detection)

Pengujian dilakukan dengan menyisipkan karakter khusus ke dalam parameter masukan untuk melihat respons sistem. Munculnya pesan kesalahan dari basis data atau perubahan perilaku aplikasi menandakan adanya celah validasi input. Teknik ini umum digunakan untuk mengidentifikasi kelemahan pada pengelolaan kueri SQL.

3. Eksploitasi (Exploitation)

Kerentanan yang terdeteksi dimanfaatkan dengan menyuntikkan perintah SQL tertentu pada parameter yang rentan. Fokus utama adalah menguji kemungkinan bypass autentikasi, yaitu melewati mekanisme login administrator tanpa kredensial sah. Tahap ini menampilkan dampak nyata dari kerentanan SQL Injection terhadap keamanan sistem dan menegaskan pentingnya validasi input serta perlindungan basis data.

Metodologi Komputasi Cerdas (Pemodelan Jaringan Saraf Tiruan)

Pendekatan ini mengembangkan model prediktif kekuatan kata sandi yang mengutamakan efisiensi dan akurasi melalui tahapan berikut:

1. Pelatihan Model

Model dilatih menggunakan data kata sandi dari insiden kebocoran keamanan nyata yang telah menjadi referensi dalam studi akademik. Proses pelatihan memungkinkan jaringan saraf untuk mengenali pola umum dalam pembuatan kata sandi, termasuk struktur, kombinasi karakter, dan tingkat kerumitan. Model ini diharapkan lebih akurat dalam mendeteksi kekuatan kata sandi dibanding metode berbasis aturan sederhana.

2. Teknik Kompresi

Setelah pelatihan, model dioptimalkan menggunakan teknik kompresi seperti kuantisasi dan pengoptimalan bobot. Tujuannya adalah mengurangi ukuran model tanpa mengurangi kinerja secara signifikan. Dengan demikian, model dapat diperkecil hingga sekitar 200 KB, sehingga dapat dijalankan pada perangkat dengan keterbatasan memori, termasuk aplikasi web dan perangkat sumber daya rendah.

3. Benchmarking

Model jaringan saraf diuji dan dibandingkan dengan model tradisional seperti Probabilistic Context-Free Grammar (PCFG) dan model Markov. Perbandingan ini bertujuan mengevaluasi kelebihan dan kekurangan masing-masing metode dalam memperkirakan kekuatan kata sandi. Hasil evaluasi digunakan sebagai tolok ukur efektivitas model jaringan saraf dalam konteks keamanan kata sandi saat ini.

Hasil dan Pembahasan

Dampak Faktor Manusia terhadap Keamanan Siber

Hasil penelitian menunjukkan bahwa faktor manusia memiliki pengaruh yang signifikan terhadap keamanan siber. Meskipun mahasiswa yang menjadi responden memiliki kecakapan digital yang memadai, kebanyakan masih cenderung menggunakan

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

kata sandi yang lemah demi kemudahan mengingat dan akses cepat. Perilaku ini menunjukkan adanya ketidakseimbangan antara pengetahuan tentang ancaman siber dan praktik keamanan yang diterapkan dalam kehidupan sehari-hari. Fenomena ini konsisten dengan teori kesadaran keamanan informasi yang menekankan bahwa pengetahuan semata tidak cukup tanpa adanya perubahan perilaku nyata.

Kelemahan dalam perilaku pengguna ini berpotensi membuka pintu bagi serangan siber seperti brute force, dictionary attack, atau credential stuffing. Oleh karena itu, penguatan kesadaran dan praktik perilaku pengguna menjadi salah satu langkah kunci dalam mitigasi risiko keamanan. Intervensi melalui pendidikan keamanan siber yang berfokus pada pembuatan kata sandi kuat, penggunaan passphrase, pengelola kata sandi, dan autentikasi multi-faktor sangat diperlukan untuk mengurangi risiko yang disebabkan oleh human error.

Efektivitas Jaringan Saraf Tiruan dalam Memodelkan Kekuatan Kata Sandi

Analisis lebih lanjut menunjukkan bahwa penerapan Jaringan Saraf Tiruan (Neural Network) dapat secara efektif memodelkan kekuatan otentikasi pada sisi klien. Dengan melatih model menggunakan dataset kata sandi nyata, jaringan saraf mampu mengenali pola pembuatan kata sandi yang umum digunakan, termasuk struktur karakter, kombinasi simbol, dan variasi subtitusi (misalnya leetspeak).

Hasil pengujian menunjukkan bahwa model ini mampu memberikan evaluasi yang lebih akurat dibandingkan metode tradisional berbasis aturan atau probabilistik, seperti PCFG dan Markov. Selain itu, teknik optimisasi model, termasuk kuantisasi dan kompresi bobot, memungkinkan model dijalankan pada perangkat dengan sumber daya terbatas, sehingga dapat diterapkan secara luas pada aplikasi berbasis web maupun perangkat klien. Pendekatan ini tidak hanya meningkatkan keamanan kata sandi, tetapi juga dapat mendukung edukasi pengguna melalui umpan balik yang jelas mengenai kekuatan kata sandi mereka.

Risiko Teknis: Kerentanan SQL Injection

Di ranah infrastruktur, pengujian teknis menunjukkan bahwa celah SQL Injection pada server web tetap menjadi risiko serius. Kerentanan ini muncul ketika aplikasi tidak melakukan validasi input dengan tepat, sehingga perintah SQL yang disisipkan oleh penyerang dapat dijalankan secara langsung pada basis data. Akibatnya, penyerang berpotensi memperoleh akses tidak sah ke data sensitif, termasuk informasi pengguna, kredensial, dan konfigurasi sistem.

Temuan ini menegaskan pentingnya penerapan praktik pengembangan yang aman, termasuk validasi dan sanitasi input secara menyeluruh, penggunaan prepared statements, serta pembatasan hak akses basis data sesuai prinsip least privilege. Penguatan sisi aplikasi dan server merupakan langkah krusial untuk mencegah eksploitasi teknis yang dapat berdampak serius pada keamanan data organisasi.

Ancaman Otomatis: Serangan Spam dan Infrastruktur

Selain faktor manusia dan kerentanan teknis, penelitian juga mengidentifikasi bahwa serangan otomatis seperti spam komentar terus berkembang. Penyerang kini memanfaatkan infrastruktur yang stabil dan bereputasi baik, misalnya forum atau situs wiki, untuk menyisipkan tautan berbahaya. Pendekatan deteksi berbasis konten menjadi kurang efektif karena isi pesan dapat bervariasi secara signifikan, sementara infrastruktur yang digunakan tetap konsisten.

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

Sistem Neightbor Watcher, yang memanfaatkan analisis graf untuk memantau kesamaan target infrastruktur, terbukti efektif dalam mendeteksi pola serangan. Metode ini memungkinkan identifikasi serangan berdasarkan hubungan dan stabilitas target, bukan hanya konten, sehingga meningkatkan akurasi deteksi dan meminimalkan false positive. Pendekatan ini menekankan pentingnya pemantauan proaktif terhadap aset strategis yang menjadi sasaran serangan siber.

Integrasi Manajemen Risiko yang Menyeluruh

Berdasarkan hasil pengujian perilaku pengguna, model prediktif kata sandi, analisis kerentanan teknis, dan deteksi serangan otomatis, dapat disimpulkan bahwa manajemen risiko keamanan siber harus diterapkan secara komprehensif. Strategi perlindungan yang efektif harus menggabungkan beberapa lapisan:

1. Penguatan Perilaku Pengguna: Meningkatkan kesadaran, pendidikan keamanan, dan penerapan praktik kata sandi yang aman.
2. Penutupan Celah Teknis: Validasi input, penggunaan prepared statement, pengaturan hak akses yang tepat, dan monitoring basis data.
3. Penerapan Algoritma Cerdas: Penggunaan model neural network untuk evaluasi kata sandi, serta sistem analisis infrastruktur seperti Neightbor Watcher untuk mendeteksi serangan otomatis.
4. Pemantauan dan Evaluasi Berkelanjutan: Menerapkan log analitik, alarm dini, dan pembaruan rutin untuk menanggapi ancaman baru yang muncul.

Pendekatan integratif ini memungkinkan organisasi untuk melindungi aset penting dan data strategis secara efektif dari ancaman siber yang semakin kompleks. Kombinasi penguatan manusia, teknologi, dan algoritma cerdas menciptakan ekosistem keamanan yang adaptif, responsif, dan berkelanjutan.

Kesimpulan

Keamanan siber yang tangguh hanya dapat dicapai melalui sinergi antara penguatan perilaku pengguna dan ketahanan infrastruktur teknologi. Meskipun literasi digital semakin meningkat, kecenderungan pengguna untuk memprioritaskan kemudahan akses dibandingkan kekuatan kriptografis masih menjadi celah utama yang perlu dimitigasi. Salah satu solusinya adalah penerapan algoritma cerdas, seperti Jaringan Saraf Tiruan, yang mampu memberikan proteksi yang efisien dan akurat di sisi klien. Di sisi infrastruktur, kerentanan teknis seperti SQL Injection, serta perkembangan serangan otomatis seperti comment spam, menuntut pengadopsian manajemen risiko yang proaktif dan penerapan sistem deteksi berbasis infrastruktur yang bersifat content-agnostic untuk meningkatkan keamanan secara menyeluruh.

Saran

Upaya pengamanan akun pengguna terhadap serangan password guessing perlu dilakukan melalui pendekatan yang tidak hanya berfokus pada teknologi, tetapi juga pada perilaku pengguna. Pengguna sebaiknya dibiasakan untuk membuat kata sandi yang kuat, unik, dan tidak digunakan secara berulang pada berbagai layanan. Dari sisi sistem, penyedia layanan perlu memperkuat mekanisme autentikasi dengan membatasi jumlah percobaan login yang gagal, menerapkan penguncian akun sementara setelah beberapa percobaan gagal, serta menambahkan lapisan verifikasi tambahan, seperti autentikasi dua faktor (2FA). Selain itu, penelitian selanjutnya disarankan untuk menggunakan variasi metode analisis dan memanfaatkan dataset yang lebih luas agar

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026

hasil yang diperoleh lebih representatif terhadap kondisi keamanan sistem di dunia nyata. Dengan penerapan langkah-langkah ini, keamanan akun pengguna dapat ditingkatkan secara signifikan, baik dari sisi perilaku manusia maupun sisi sistem teknologi.

Daftar Pustaka

Sopandi, D., Sukarno, P., & Yasirandi, R. (2021). Evaluasi dan Analisis Security Awareness dalam Password Behavior pada Mahasiswa. e- Proceeding of Engineering, Vol. 8, No. 5, Oktober 2021, Hal. 11488-11500. Bandung: *Universitas Telkom*.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen, Vol. 1, No. 2, Juni 2023, Hal. 172-191. Jakarta: *Universitas Bhayangkara Jakarta Raya*.

Melicher, W., Ur, B., Segreti, S. M., Komanduri, S., Bauer, L., Christin, N., & Cranor, L. F. (2016). Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks. In Proceedings of the 25th USENIX Security Symposium, August 10-12, 2016, Hal. 1-18. Austin, TX: Carnegie Mellon University.

Rumaf, N., Anwar, K., & Utsalina, D. S. (2013). Analisis Keamanan Web Server Terhadap Website PT. Victory Internasional Futures Malang Dengan Teknik SQL Injection. Jurnal Penelitian Teknik Informatika, STIMATA Malang.

Zhang, J., & Gu, G. (2014). NEIGHBOR WATCHER: A Content-Agnostic Comment Spam Inference System. SUCCESS Lab, Department of Computer Science & Engineering. College Station, TX: *Texas A&M University*.

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. Jurnal Surya Kencana Data: Dinamika Masalah Hukum dan Keadilan, Vol. 5, No. 2, Hal. 577-592.

Weir, M., Aggarwal, S., Medeiros, B. D., & Glodek, B. (2009). Password cracking using probabilistic context-free grammars. IEEE Symposium on Security and Privacy.

Received: November 18, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 10, 2026