JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8183

SIMULASI HASHING PASSWORD MENGGUNAKAN ARGON2 DAN SCRYPT SERTA PENGEMBANGAN FITUR LOGGING JARINGAN REAL-TIME BERBASIS WEBSITE

Nezza Anggraini Yolandari[1], Dedy Kiswanto[2], Sherly Davina[3], Ahmad Denil Sitepu[4]

[1234] Ilmu Komputer, Universitas Negeri Medan, Jl. Willem Iskandar Pasar V, Medan Estate, Sumatera Utara, 20221.

Keywords:
Argon2; Scrypt; Password Hashing; Real-Time Logging; Network Security.

Corespondent Email:
nezzaanggraini0@gmail.com

Abstrak. Penelitian ini mengembangkan sistem keamanan berbasis website dengan mengintegrasikan algoritma hashing Argon2 dan Scrypt serta sistem logging jaringan real-time menggunakan WebSocket (Ratchet PHP). Tujuan utama penelitian ini adalah mensimulasikan keamanan penyimpanan password sekaligus memantau aktivitas jaringan secara langsung untuk mendeteksi anomali. Metode yang digunakan adalah eksperimen melalui simulasi login, hashing, serta deteksi serangan ARP Poisoning pada lingkungan lokal (localhost). Hasil pengujian menunjukkan bahwa Argon2 memiliki waktu hashing lebih cepat dengan tingkat keamanan tinggi, sedangkan Scrypt menawarkan efisiensi memori yang baik. Sistem berhasil mendeteksi serangan ARP Poisoning dalam waktu kurang dari satu detik dan melakukan pemblokiran IP secara otomatis. Kesimpulannya, integrasi hashing dan logging real-time ini efektif meningkatkan keamanan jaringan berbasis website. Ke depannya, sistem dapat dikembangkan ke dalam lingkungan cloud atau IoT untuk perluasan fungsi monitoring.

Abstract. *This study is development of a web-based security system integrating the Argon2 and Scrypt hashing algorithms with a real-time network logging system using WebSocket (Ratchet PHP). The main objective is to simulate secure password storage while monitoring network activity in real time to detect anomalies. The research method employed an experimental simulation of login, hashing, and ARP Poisoning attack detection in a local environment (localhost). The results indicate that Argon2 provides faster hashing time and higher security, while Scrypt offers better memory efficiency. The system successfully detected ARP Poisoning attacks in less than one second and automatically blocked the attacker's IP address. In conclusion, the integration of hashing and real-time logging effectively enhances web-based network security. Future development may include integration with cloud or IoT environments to expand monitoring capabilities.*

1. PENDAHULUAN

Keamanan jaringan menjadi aspek penting di era digital. Pesatnya perkembangan teknologi informasi memicu pertumbuhan layanan berbasis internet yang turut meningkatkan ancaman siber yang dapat mengganggu ketersediaan, kerahasiaan, serta integritas data [1]. Seiring bergesernya berbagai transaksi dan layanan ke media daring, terjadi pula peningkatan kasus kriminalitas di internet, termasuk insiden kebocoran data penting seperti kata sandi [2]. Keamanan penyimpanan data pengguna merupakan aspek yang sangat penting dalam sebuah sistem informasi berbasis website [3]. Salah satu langkah preventif yang paling mendasar untuk menghindari peretasan kata sandi adalah dengan menerapkan hashing pada penyimpanan password [2]. Fungsi hash yang baik akan mengubah data menjadi sebuah nilai representasi (nilai hash) agar data yang dimaksud tidak dapat dengan mudah diretas dan disalahgunakan oleh pihak yang tidak berwenang [4]. Namun, tidak semua algoritma hashing benar-benar aman dari berbagai metode

peretasan. Algoritma hashing tradisional seperti MD5 atau SHA-256 seringkali rentan terhadap serangan Brute Force dan Dictionary Attack karena kecepatannya dalam memproses hash [5]. Sebagai contoh, Bcrypt menunjukkan ketahanan yang baik terhadap Brute Force Attack dibandingkan algoritma hashing lainnya [3], [6]. Untuk mengatasi tantangan keamanan ini, diperlukan penggunaan fungsi turunan kunci berbasis kata sandi (Password-Based Key Derivation Function/PBKDF) yang dirancang secara khusus untuk memperlambat proses hashing, seperti Argon2 dan Scrypt.

Argon2 merupakan pemenang Password Hashing Competition (PHC) pada tahun 2015 dan dirancang untuk mengutamakan kecepatan waktu, penggunaan memori, dan tingkat paralelisme [7]. Argon2 direkomendasikan karena menunjukkan keseimbangan terbaik antara keamanan dan kinerja, serta sangat resisten terhadap serangan berbasis perangkat keras seperti GPU dan ASIC [8]. Algoritma ini sengaja dibuat intensif memori dan waktu komputasi, menjadikannya sangat resisten terhadap serangan berbasis perangkat keras [6].

Scrypt dirancang dengan konsep memory-hard function, yang membutuhkan kapasitas memori besar untuk menghasilkan hash, sehingga menyulitkan proses brute force menggunakan perangkat keras paralel seperti GPU atau ASIC. Scrypt lebih menekankan pada kompleksitas memori untuk memperlambat serangan [11]. Oleh karena itu, penelitian ini menggunakan keduanya untuk melakukan simulasi komparatif, agar dapat menilai perbedaan tingkat keamanan dan efisiensi antara dua algoritma hashing kuat dengan pendekatan perlindungan yang berbeda.

Selain keamanan penyimpanan kata sandi, sistem juga memerlukan kemampuan pemantauan keamanan jaringan secara real-time. Diperlukan sebuah sistem log yang bersifat real-time dan fleksibel agar pengguna dapat melakukan monitoring perangkat dengan mudah. Data logging bertujuan untuk mencatat setiap kondisi atau peristiwa yang terjadi dalam sistem [9]. Pengembangan real-time monitoring dan data logging berbasis web telah terbukti dapat meningkatkan efisiensi operasional dan mengurangi kesalahan manusia [10]. Kombinasi antara keamanan password yang kuat dan visibilitas aktivitas jaringan yang real-time akan meningkatkan integritas dan kepercayaan pengguna terhadap layanan berbasis website [11].

Penelitian ini bertujuan untuk melakukan simulasi komparatif antara algoritma hashing Argon2 dan Scrypt dalam mengamankan password, dan mengintegrasikan hasil simulasinya ke dalam sebuah sistem logging jaringan real-time berbasis website. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi implementasi algoritma hashing terbaik yang dikombinasikan dengan sistem monitoring keamanan yang efektif.

2. TINJAUAN PUSTAKA

2.1 Keamanan Data dan Fungsi Hashing

Keamanan data merupakan aspek yang sangat penting dalam sistem informasi [2]. Implementasi ilmu kriptografi menjadi semakin sering digunakan seiring dengan daruratnya keamanan data [4]. Di dalam ilmu kriptografi, fungsi hash (fungsi satu arah) digunakan untuk mengubah data menjadi nilai representasi, sehingga data tersebut tidak dapat dengan mudah diretas [4]. Fungsi hash yang aman memberikan kemungkinan untuk menyimpan password secara aman karena inputnya tidak dapat diperoleh kembali [10]. Fungsi Turunan Kunci Berbasis Kata Sandi (PBKDF) Lanjutan Untuk melawan kecepatan algoritma hashing tradisional yang tinggi (yang menjadi kelemahan karena memudahkan serangan Brute Force oleh peretas yang menggunakan perangkat keras canggih [3], [5], dikembangkanlah fungsi hashing yang sengaja diperlambat (PBKDF). PBKDF ini dirancang dengan membuat prosesnya intensif memori dan waktu komputasi [12].

2.2 Algoritma Hashing untuk Keamanan Password

Algoritma hashing yang efektif harus mampu menahan berbagai metode peretasan. Argon2 merupakan algoritma hashing paling unggul saat ini dan menjadi pemenang PHC [6]. Argon2 dirancang sebagai fungsi memory-hard yang sangat resisten terhadap serangan berbasis GPU/ASIC [7]. Argon2 menawarkan tiga parameter utama (time cost, memory cost, parallelism) yang dapat disesuaikan untuk mengoptimalkan keamanan dan kinerja [7]. Dan Scrypt adalah algoritma hashing yang bersifat *memory-hard*, artinya membutuhkan memori besar saat proses hashing sehingga sulit

diserang dengan brute force menggunakan GPU atau ASIC. Algoritma ini mengubah password menjadi hash unik melalui proses pencampuran data berulang, menjadikannya cepat namun tetap aman untuk penyimpanan password. Algoritma ini dapat menjadi alternatif yang kuat di sistem di mana Argon2 belum tersedia [11]. Terdapat juga berbagai algoritma hashing lain yang umum digunakan:

a. Bcrypt: adalah salah satu algoritma yang dinyatakan cukup efektif untuk mengamankan password dari berbagai metode peretasan [2]. Implementasi Bcrypt telah digunakan untuk mengenkripsi dan meng-hash data pengguna pada website [3]. Analisis kinerja Bcrypt juga menunjukkan performa yang baik untuk meningkatkan keamanan password dari serangan Brute Force [6].
b. SHA-512: Merupakan bagian dari keluarga Secure Hashing Algorithm (SHA) yang digunakan untuk otentikasi pengguna pada halaman sign-up sistem berbasis website [13].
c. SHA-256 dan MD5: Keduanya adalah fungsi hash yang umum. Hasil perbandingan menunjukkan bahwa fungsi hash SHA256 lebih baik dalam mengamankan data dibandingkan MD5 [4]. Namun, algoritma seperti MD5 dan SHA-256 memiliki ketahanan yang lebih rendah terhadap Brute Force Attack dibandingkan PBKDF [3], [5].

2.3 Data Logging dan Monitoring Real-Time Berbasis Website serta Deteksi Anomali

Data logging bertujuan untuk mencatat setiap kondisi atau peristiwa yang terjadi pada sebuah alat atau sistem secara otomatis dan berurutan [8]. Tujuannya adalah untuk memantau kondisi sistem, mendeteksi anomali, serta menyediakan jejak audit atas setiap tindakan yang dilakukan. Sistem log yang dibutuhkan harus bersifat real-time dan fleksibel agar pengguna dapat melakukan monitoring perangkat dengan mudah [9], [8]. Pengembangan real-time monitoring dan data logging berbasis web telah diterapkan pada berbagai kasus untuk meningkatkan efisiensi dan keamanan [9]. Perkembangan ini mendorong solusi navigasi yang real-time, tidak bergantung pada aplikasi native, dan memiliki antarmuka visual yang responsif tetapi ringan dijalankan pada perangkat dengan spesifikasi terbatas [16]. Dalam konteks keamanan jaringan, logging dan monitoring real-time ini sangat penting untuk Deteksi Anomali. Deteksi anomali melibatkan pengawasan pola komunikasi jaringan yang tidak biasa, yang merupakan indikasi serangan siber [10].

2.4 Deteksi Anomaly ARP Poisoning

Serangan ARP Poisoning adalah bentuk serangan Man-in-the-Middle (MITM) di mana penyerang mengirimkan frame ARP palsu untuk mengalihkan lalu lintas. Deteksi anomali ARP poisoning dilakukan dengan memantau ketidaksesuaian antara pasangan IP dan MAC Address. Jika satu IP terdeteksi memiliki dua MAC berbeda, sistem mengidentifikasinya sebagai serangan ARP poisoning. Deteksi ini memanfaatkan kelemahan ARP yang tidak memiliki mekanisme verifikasi sumber, sehingga memungkinkan pemetaan IP–MAC palsu dikirim oleh penyerang [15]. Sistem monitoring jaringan real-time yang dikombinasikan dengan protokol seperti ICMP [14] dan analisis log dapat mendeteksi lalu lintas mencurigakan yang mengindikasikan serangan MITM (seperti ARP Poisoning) atau anomali lainnya [15].

3. METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian ini menggunakan metode eksperimen dengan melakukan simulasi sistem keamanan berbasis web yang memanfaatkan algoritma hashing Argon2 dan Scrypt untuk proses pengamanan password, serta websocket (Ratchet PHP) untuk melakukan pencatatan dan pemantauan aktivitas jaringan secara real-time.

Tujuan utama rancangan ini adalah menguji efektivitas sistem dalam mencatat aktivitas user dan mendeteksi anomali jaringan (serangan ARP poisoning) melalui dashboard admin. Sistem diuji dalam dua kondisi utama: kondisi normal, ketika user melakukan login dengan IP dan MAC Address yang valid. Dan kondisi anomali, ketika terdapat dua MAC Address berbeda yang menggunakan IP Address sama, sehingga sistem memberikan notifikasi serangan dan melakukan pemblokiran IP secara otomatis.

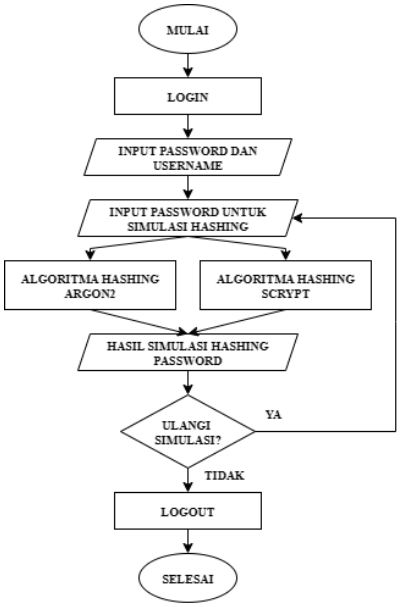
Penelitian dikembangkan menggunakan pendekatan simulasi berbasis sistem

terintegrasi, di mana peneliti membuat, menjalankan, dan menguji aplikasi web secara langsung di lingkungan lokal (localhost) menggunakan XAMPP sebagai server utama.

3.2 Perancangan Sistem

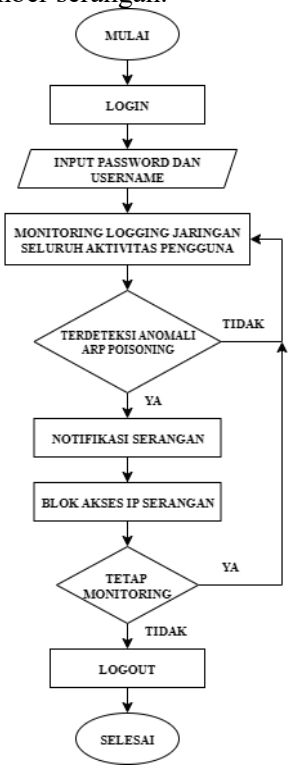
Sistem yang dibangun terdiri atas beberapa komponen utama. Frontend menggunakan HTML, CSS, dan JavaScript untuk membangun tampilan antarmuka yang interaktif dan responsif bagi pengguna. Pada sisi backend, digunakan PHP sebagai logika utama sistem yang mengatur alur proses, manajemen data, serta pengelolaan WebSocket server. Komponen database memanfaatkan MySQL untuk menyimpan berbagai data penting, seperti informasi pengguna, log aktivitas, serta riwayat pemblokiran jaringan. Selain itu, sistem juga dilengkapi dengan WebSocket server yang dijalankan menggunakan Ratchet PHP, berfungsi sebagai penghubung antara client (user atau admin) dan server, sehingga memungkinkan terjadinya komunikasi dua arah secara real-time.

Sistem dirancang berbasis website dengan struktur dua peran utama, yaitu user dan admin. User melakukan registrasi akun serta login menggunakan username dan password yang sesuai. User dapat melakukan simulasi hashing password menggunakan 2 algoritma berbeda, yaitu Argon2 dan Scrypt. Seluruh aktivitas user akan di kirim ke dahsboard admin.



Gambar 1. Alur sistem user

Admin dapat melihat seluruh aktivitas user yang tercatat melalui dashboard monitoring yang diperbarui secara real-time. Admin dapat menerima notifikasi serangan ARP Poisoning jika ditemukan IP Address yang memiliki dua MAC Address yang berbeda. Admin dapat melakukan pemblokiran IP yang terindikasi sebagai sumber serangan.



Gambar 2. Alur sistem admin

3.3 Teknik Pengumpulan Data

Data dalam penelitian dikumpulkan melalui simulasi dan observasi langsung terhadap aktivitas sistem selama proses pengujian berlangsung. Jenis data yang diperoleh meliputi beberapa kategori, yaitu data log aktivitas yang mencatat informasi seperti waktu, tanggal, username, role, action, IP Address, dan MAC Address; data respon sistem yang mencakup hasil hashing password, status login, notifikasi serangan, serta aktivitas real-time yang ditampilkan pada dashboard admin; dan data hasil pengujian yang berisi perbandingan perilaku sistem pada kondisi normal maupun saat terjadi serangan. Seluruh proses pengumpulan data dilakukan secara otomatis oleh sistem dan disimpan dalam database MySQL, kemudian hasilnya diamati serta dianalisis melalui tampilan dashboard website.

3.4 Sumber Data Penelitian

Penelitian ini tidak melibatkan partisipan manusia secara langsung. Sumber data berasal dari simulasi yang dibangun menghasilkan data aktivitas (log) selama proses login, hashing, dan komunikasi jaringan serta skenario simulasi yang dijalankan oleh peneliti, baik sebagai user maupun admin, untuk menguji fungsi sistem dan deteksi anomali.

3.5 Teknik Analisis Data

Analisis data dalam penelitian ini dilakukan secara deskriptif untuk memahami kinerja serta efektivitas sistem yang dikembangkan. Tahapan analisis meliputi beberapa aspek utama. Analisis fungsi hashing dilakukan dengan menilai hasil hashing password menggunakan Argon2 dan Scrypt, untuk melihat tingkat keberhasilan proses hashing serta perbedaan hasil enkripsi yang dihasilkan oleh masing-masing algoritma. Analisis logging real-time dilakukan untuk mengamati efektivitas WebSocket dalam menampilkan aktivitas pengguna secara langsung pada dashboard admin.

Analisis deteksi anomali bertujuan untuk menguji kemampuan sistem dalam mendeteksi dan memberikan notifikasi terhadap aktivitas mencurigakan, seperti adanya satu IP Address yang terdeteksi memiliki dua MAC Address berbeda. Analisis pemblokiran IP dilakukan untuk mengevaluasi respon sistem terhadap tindakan admin dalam memblokir IP yang terindikasi sebagai sumber serangan, serta memastikan bahwa proses logging dapat kembali berjalan normal setelah pemblokiran dilakukan.

3.6 Pengujian Sistem

Pengujian sistem dilakukan melalui tiga skenario utama untuk menilai kinerja dan respon sistem terhadap berbagai kondisi jaringan. Pada kondisi normal, pengguna melakukan login menggunakan IP Address dan MAC Address yang valid, di mana sistem diharapkan dapat mencatat seluruh aktivitas secara normal tanpa adanya anomali. Kemudian kondisi anomali (ARP Poisoning) dilakukan dengan menghadirkan pengguna yang mencoba login menggunakan IP Address yang sama namun dengan MAC Address berbeda. Sistem harus mampu mendeteksi adanya anomali jaringan dan menampilkan notifikasi serangan secara real-time pada dashboard admin.

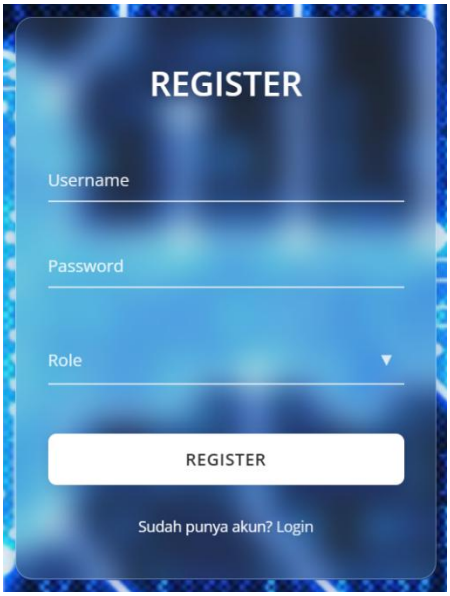
Terakhir pada kondisi pemulihan sistem, admin melakukan tindakan pemblokiran terhadap IP yang terindikasi sebagai sumber serangan. Setelah proses pemblokiran berhasil, sistem diharapkan dapat kembali berfungsi normal dan mencatat aktivitas baru tanpa gangguan, menunjukkan keberhasilan mekanisme pemulihan yang diterapkan.

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Implementasi sistem dilakukan dengan membangun sebuah website yang mengintegrasikan proses simulasi hashing password menggunakan algoritma Argon2 dan Scrypt, serta logging aktivitas jaringan secara real-time menggunakan WebSocket (Ratchet PHP). Sistem terdiri atas dua peran utama, yaitu user dan admin, dengan fungsi yang saling berhubungan dalam satu basis data dan server komunikasi real-time.

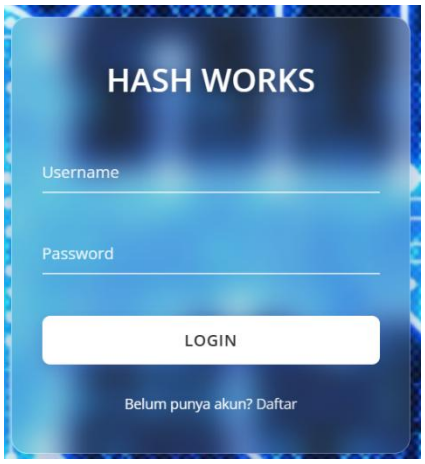
Berikut ini merupakan hasil implementasi antarmuka dan fungsi utama sistem:



Gambar 3. Register page

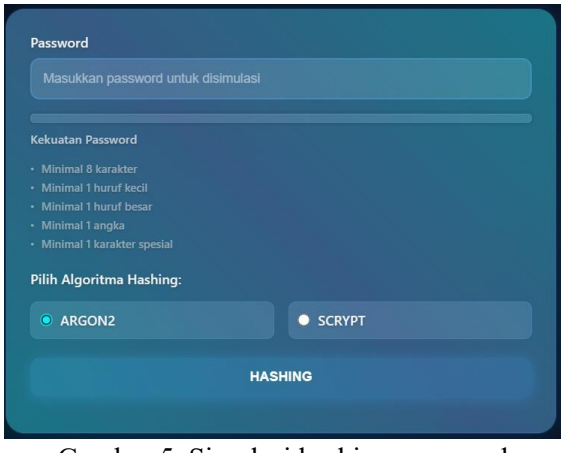
Halaman ini digunakan oleh pengguna baru untuk membuat akun sebelum dapat melakukan login. Pada halaman registrasi, pengguna diminta untuk mengisi username, password, serta role. Proses ini akan mengaktifkan fungsi hashing untuk menyimpan password ke database dengan aman sebelum data dikirim.

Selain itu, sistem juga melakukan pencatatan aktivitas registrasi seperti waktu, IP Address, dan MAC Address pengguna, yang dikirim secara real-time ke dashboard admin.



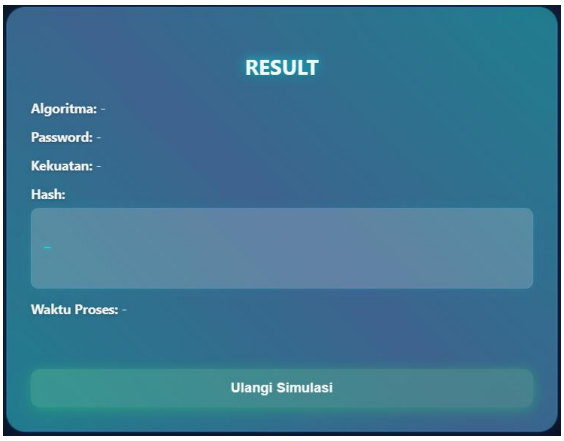
Gambar 4. Login page

Pada halaman login, pengguna memasukkan username dan password yang telah terdaftar. Sistem kemudian memverifikasi kredensial tersebut dengan mencocokkan hash password di database. Jika login berhasil, sistem mencatat aktivitas login ke dalam log real-time, termasuk IP Address dan MAC Address pengguna. Data ini dikirim ke dashboard admin agar admin dapat memantau setiap sesi login yang terjadi, mendeteksi duplikasi IP, serta mengidentifikasi potensi serangan jaringan.



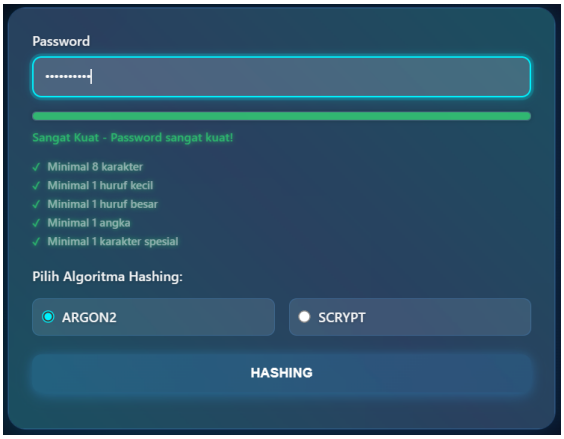
Gambar 5. Simulasi hashing password

Setelah berhasil login, pengguna diarahkan ke dashboard utama yang menyediakan fitur simulasi hashing. Pada bagian ini, user dapat memilih algoritma hashing (Argon2 atau Scrypt) dan memasukkan teks password yang ingin diuji. Sistem kemudian akan menampilkan hasil hashing serta waktu proses hashing secara langsung, sehingga pengguna dapat memahami perbedaan efisiensi dan tingkat keamanan dari kedua algoritma tersebut.



Gambar 6. Hasil hashing password

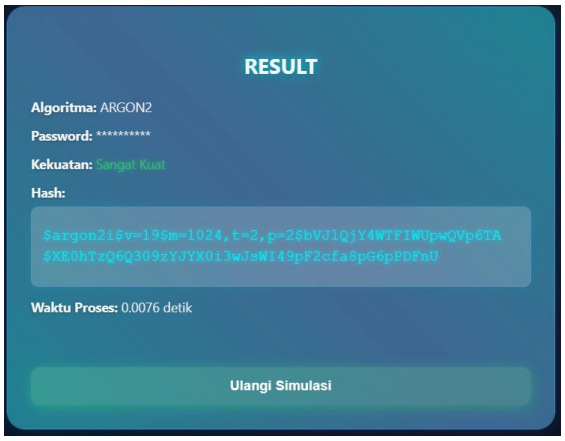
Setelah proses hashing dilakukan, hasil enskripsi password ditampilkan secara lengkap. informasi yang ditampilkan meliputi password asli (input user), algoritma yang digunakan, nilai hash yang dihasilkan, dan durasi waktu hashing. Data ini juga dikirim ke database dan tercatat dalam log aktivitas, yang dapat diakses oleh admin secara real-time melalui dashboard monitoring.



Gambar 7. Input simulasi hashing password

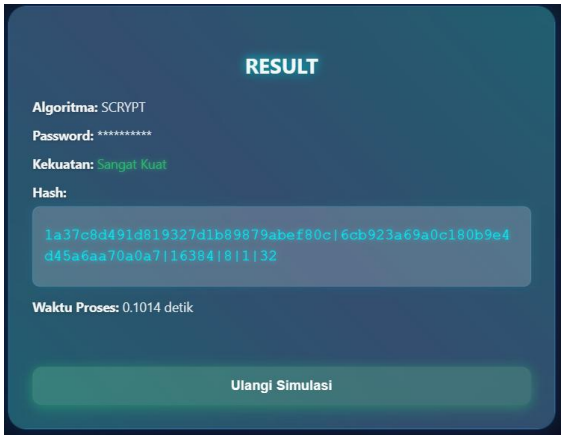
Fitur tambahan pada dashboard user adalah pengujian kekuatan password. Saat pengguna mengetik password, sistem otomatis menilai tingkat keamanannya berdasarkan panjang karakter, kombinasi huruf besar/kecil, angka, dan simbol. Hasil evaluasi ditampilkan dalam bentuk indikator seperti “Sangat Lemah”,

"Lemah", "Sedang", "Kuat" dan "Sangat Kuat", yang membantu pengguna memahami pentingnya pembuatan password yang kompleks sebelum dilakukan hashing.



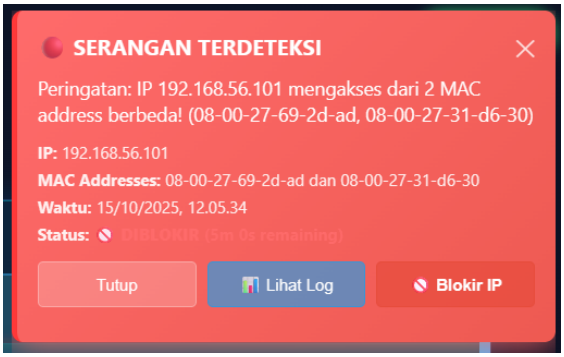
Gambar 8. Hasil Hashing dengan Argon2

Ketika pengguna memilih algoritma Argon2, sistem menampilkan hasil hash yang unik dan kompleks. Argon2 memiliki keunggulan pada sisi resistensi terhadap serangan brute force dan penggunaan memori yang dapat diatur, sehingga hasil hash akan berbeda meskipun password input sama namun salt berbeda. Hasil implementasi menunjukkan hashing Argon2 membutuhkan waktu sedikit lebih cepat dibanding Scrypt, dan memberikan tingkat keamanan yang tinggi.



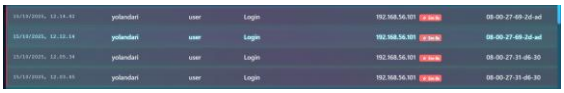
Gambar 9. Hasil hashing dengan Scrypt

Pada algoritma Scrypt, hasil hashing juga ditampilkan dengan nilai hash panjang dan acak. Scrypt memiliki keunggulan dari sisi efisiensi dan kecepatan hashing yang lebih tinggi dibanding Argon2, namun dengan tingkat keamanan yang tetap kuat terhadap serangan brute force berbasis hardware. Hasil simulasi menunjukkan perbedaan durasi waktu hashing yang signifikan, menegaskan bahwa Scrypt sedikit lebih lama namun Argon2 lebih tahan terhadap serangan berbasis paralel komputasi.



Gambar 10. Notifikasi deteksi anomali

Sistem dilengkapi dengan fitur deteksi serangan ARP Poisoning. Jika sistem menemukan dua MAC Address berbeda menggunakan IP Address yang sama, maka dashboard admin akan langsung menampilkan notifikasi serangan secara real-time. Notifikasi ini muncul dalam bentuk pop-up peringatan serta perubahan warna pada tabel log (misalnya menjadi merah), yang menandakan adanya aktivitas anomali pada jaringan.



Gambar 11. log aktivitas anomali

Setiap aktivitas mencurigakan tercatat dalam log jaringan yang mencantumkan waktu kejadian, IP Address penyerang, MAC Address yang terdeteksi ganda, serta status aktivitas. Log ini membantu admin melacak sumber serangan dan menganalisis pola aktivitas jaringan yang tidak normal.

Gambar 12. Log normal

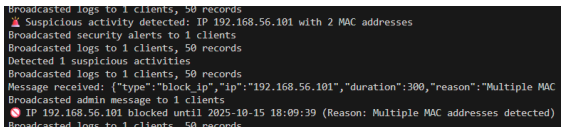
Pada kondisi normal, log aktivitas menunjukkan informasi rutin seperti username,

IP Address dan MAC Address, aktivitas, status koneksi, dan waktu akses. Data log ini mengalir secara real-time dan tidak menampilkan notifikasi peringatan. Hal ini menandakan bahwa sistem bekerja dalam kondisi stabil tanpa adanya gangguan jaringan.

Gambar 13. Blokir IP serangan

Ketika terdeteksi IP yang terindikasi sebagai sumber serangan, admin dapat menekan tombol “Blokir IP” pada dashboard. Fitur ini mengirimkan perintah otomatis ke sistem backend untuk menambahkan IP tersebut ke dalam daftar blokir (blacklist).

IP diblokir dengan perintah ***netsh advfirewall firewall add rule name="Block_VM_IP" dir=in and out action=block remoteip=(IP serangan)***. Setelahnya diuji dengan melakukan ping ke IP serangan tersebut. Maka ping tersebut gagal yang menandakan bahwa user dari IP tersebut tidak dapat mengakses sistem lagi. Untuk membuka blokir jalankan perintah ***netsh advfirewall firewall delete rule name="Block_VM_IP"***. Maka akses sistem diizinkan kembali.



Gambar 14. Terminal saat ada serangan

Hasil keluaran terminal dari WebSocket server yang menunjukkan adanya deteksi aktivitas anomali pada jaringan. Berdasarkan tampilan tersebut, sistem mendeteksi satu IP Address yang digunakan oleh dua MAC Address berbeda. Kondisi ini merupakan indikasi dari serangan ARP Poisoning, di mana penyerang mencoba melakukan penyamaran dengan memalsukan alamat MAC untuk IP yang sama guna mengacaukan tabel ARP pada jaringan. Terlihat pada terminal bahwa sistem mengirimkan pesan dengan tipe "block_ip" yang berisi informasi IP target, dan alasan pemblokiran yaitu “Multiple MAC addresses detected”.

4.2 Hasil Pengujian

Pengujian sistem dilakukan berdasarkan tiga kondisi berbeda, yaitu:

1. Pada kondisi normal, user melakukan login dengan IP dan MAC Address yang valid. Hasil pada sistem menunjukkan bahwa sistem mampu mencatat seluruh aktivitas seperti login, hashing, dan logout dengan status normal tanpa adanya notifikasi serangan. Log data tampil stabil di dashboard admin secara real-time.
2. Pada kondisi serangan (ARP Poisoning), Ketika dua perangkat menggunakan IP Address yang sama dengan MAC Address berbeda, sistem berhasil mendeteksi anomali. Admin menerima notifikasi serangan dalam waktu kurang dari satu detik, dan data log menunjukkan IP serta MAC Address yang terlibat. Hasil ini membuktikan bahwa algoritma deteksi berbasis perbandingan IP–MAC berjalan efektif dan dapat diandalkan untuk mendeteksi ARP poisoning.
3. Pada kondisi pemulihan dan pemblokiran IP, admin melakukan pemblokiran terhadap IP yang terindikasi menyerang. Setelah pemblokiran, sistem kembali berjalan normal dan aktivitas baru dapat tercatat tanpa gangguan. Proses pemblokiran terbukti mampu mencegah akses ulang dari IP yang sama, memastikan integritas sistem tetap terjaga.

5. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem keamanan berbasis website yang mengintegrasikan algoritma hashing Argon2 dan Scrypt dengan fitur logging jaringan real-time menggunakan WebSocket (Ratchet PHP). Sistem mampu mencatat aktivitas pengguna secara langsung, mendeteksi serangan ARP Poisoning, serta melakukan pemblokiran IP otomatis secara efektif. Berdasarkan hasil penelitian dapat disimpulkan:

1. Argon2 menunjukkan waktu hashing lebih cepat dan tingkat keamanan tinggi, sedangkan Scrypt memiliki efisiensi

memori yang baik meski sedikit lebih lambat.
2. Sistem logging real-time berfungsi optimal dalam menampilkan aktivitas jaringan dan notifikasi anomali secara langsung.
3. Mekanisme deteksi dan pemblokiran serangan berjalan efektif dan menjaga stabilitas sistem setelah pemulihan.
4. Kelebihan sistem terletak pada integrasi keamanan password dan monitoring jaringan dalam satu platform. Kekurangannya adalah masih terbatas pada uji lingkungan lokal (localhost).
5. Pengembangan berikutnya dapat diarahkan pada integrasi dengan cloud atau IoT serta penambahan modul analisis serangan berbasis machine learning.

UCAPAN TERIMA KASIH

Tim penulis mengucapkan puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penelitian dengan judul *"Simulasi Hashing Password Menggunakan Argon2 dan Scrypt Serta Pengembangan Fitur Logging Jaringan Real-Time Berbasis Website"* ini dapat diselesaikan dengan baik. Ucapan terima kasih penulis sampaikan kepada dosen pembimbing yang telah memberikan arahan, motivasi, serta masukan yang sangat berharga selama proses penelitian ini berlangsung. Terima kasih juga disampaikan kepada rekan-rekan satu tim yang telah membantu dalam proses pengembangan sistem, pengujian, serta diskusi teknis yang mendukung kelancaran penelitian ini. Tim Penulis menyadari bahwa penelitian ini masih memiliki keterbatasan, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk penyempurnaan karya di masa mendatang.

DAFTAR PUSTAKA

[1] D. Kiswanto, F. Ramadhani, N. M. Surbakti, and N. A. Nasution, "Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest," Buletin of Information Technology (BIT), vol. 6, no. 3, 2025.

[2] R. M. Liauren, B. Zaman, dan S. Bahri, "Implementasi Algoritma Aes Dan Bcrypt Untuk Pengamanan Data Pengguna Pada Website Jahitku," Jurnal Kharisma Tech, vol. 20, no. 01, hlm. 57–71, 2025.

[3] M. R. Firdaus, "Analisis Penggunaan Algoritma Bcrypt dengan Garam (Salt) untuk Pengamanan Password dari Peretasan," Makalah-Matdis-2021 (48).pdf, 2021.

[4] I. Rahim, N. Anwar, A. M. Widodo, K. K. Juman, dan I. Setiawan, "Komparasi Fungsi Hash Md5 Dan Sha256 Dalam Keamanan Gambar Dan Teks," IKRAITH-Informatika, 2022.

[5] I. G. A. S. Mahendra, I N. A. Jaya, dan I G. M. A. Wibawa, "Analisis Kinerja Algoritma Hashing SHA-256 dan MD5 untuk Keamanan Password pada Aplikasi Web," Jurnal Ilmiah Teknologi dan Elektro (JITET), vol. 2, no. 1, hlm. 1–8, 2023.

[6] S. Suendri, "Hashing Argon2 Untuk Keamanan Password Pada Sistem Berbasis Web Menggunakan PHP," JISTech, vol. 4, no. 1, hlm. 46, 2019.S. Suendri, "Hashing Argon2 Untuk Keamanan Password Pada Sistem Berbasis Web Menggunakan PHP," JISTech, vol. 4, no. 1, hlm. 46, 2019.

[7] O. Kolomiytsev, V. Komarov, A. Katunin, dan D. Zemlyanskyi, "Password Hashing Methods And Algorithms On The .Net Platform," Advanced Information Systems, vol. 8, no. 4, hlm. 82–92, 2024.

[8] D. P. Nur'Aini dan S. Lestari, "Analisis Performa Transmisi Data Log Berbasis IoT Cloud Pada Kunci Pintu Pintar Menggunakan Rekognisi Wajah," IJAI (Indonesian Journal of Applied Informatics), vol. 7, no. 1, 2022.

[9] R. Maududy dan D. R. Nursamsi, "Pengembangan Real-Time Monitoring dan Data Logging Berbasis Web Pada Proses Robot Painting untuk Meningkatkan Efisiensi Produksi," Informatics And Digital Expert (Index), vol. 5, no. 2, hlm. 89–94, 2023.

[10] A. R. R. Umar, I. Busthomi, dan A. W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks," Register: Jurnal Ilmiah Teknologi Sistem Informasi, vol. 8, no. 1, hlm. 1–9, 2022.

[11] R. K. Siregar dan W. O. H. P. Sari, "Perancangan Sistem Keamanan Otentikasi Password Menggunakan Algoritma Argon2 Pada Web Service," Jurnal Media Informatika Budidarma, vol. 7, no. 3, hlm. 1386–1391, 2023.

[12] T. P. Batubara, S. Efendi, dan E. B. Nababan, "Analysis Performance Bcrypt Algorithm to Improve Password Security from Brute Force," in Journal of Physics: Conference Series, IOP Publishing Ltd, 2021.

[13] C. Agusniar, I. Fazira, dan L. Wahyunita, "Implementation of the Secure Hashing Algorithm-512 (SHA-512) for Sign-Up Page Security in the KelasSeru Tutoring System," Journal of Advanced Computer Knowledge and Algorithms (JACKA), vol. 2, no. 1, hlm. 19–23, 2025.

[14] P. Pratama, M. A. A. Mustadi, dan D. F. Iriana, "Sistem Monitoring Jaringan Realtime Berbasis Internet Control Message Protocol," JINTECH: Journal of Information Technology, vol. 3, no. 2, hlm. 67–80, 2022.

[15] A. A. Galal, A. Z. Ghalwash, and M. M. Nasr, "A New Approach for Detecting and Mitigating Address Resolution Protocol (ARP) Poisoning," International Journal of Advanced Computer Science and Applications, vol. 13, no. 6, 2022.

[16] T. Taufiqurrahman, S. E. Simatupang, R. Ramadhansyah, I. C. Sari, dan I. Rafli, "Navigasi Realtime Menggunakan Incremental GPS Path Logging Algorithm dan Visualisasi Interaktif Berbasis Web," Jurnal Minfo Polgan, vol. 14, no. 1, hlm. 1340–1354, 2025.