JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3S1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3S1.8133

IMPLEMENTASI SISTEM KEAMANAN WEBSITE DENGAN ANALISIS LOG DAN DETEKSI AKTIVITAS ANOMALI MENGGUNAKAN ISOLATION FOREST

Delvita Aulia Artika[1], Daniel Rumahorbo[2], Muhammad haikal Al – Majid[3], Dedy Kiswanto[4]

[1,2,3,4]Ilmu Komputer, Universitas Negeri Medan, Jl. Williem Iskandar Pasar V, Medan Estate, Medan, Sumatera Utara, 20221

Keywords:
Keamanan website;
Analisis Log;
Deteksi Anomali;
Isolation Forest; OTP Telegram.

Corespondent Email:
xxxxxxxxxx@kampus.ac.id

Abstrak. *Keamanan website merupakan aspek penting dalam menjaga integritas, ketersediaan, dan kepercayaan pengguna terhadap layanan digital. Penelitian ini bertujuan mengimplementasikan sistem keamanan website berbasis analisis log dan deteksi aktivitas anomali menggunakan algoritma Isolation Forest. Sistem yang dikembangkan, bernama SecurityShield, mencatat seluruh aktivitas pengguna seperti login, logout, dan registrasi ke dalam database log, kemudian menganalisisnya untuk mendeteksi aktivitas mencurigakan secara real-time. Proses deteksi dilakukan melalui tiga parameter utama yaitu Request Rate Analysis, Brute-Force Detection, dan Temporal Anomaly Detection, dengan hasil ditampilkan melalui dashboard interaktif berbasis WebSocket. Pengujian model menunjukkan nilai precision sebesar 80%, recall 8,7%, F1-score 15,7%, dan akurasi 57%, yang menandakan tingkat ketepatan tinggi namun sensitivitas masih rendah. Hasil penelitian menunjukkan bahwa penerapan Isolation Forest efektif dalam mendeteksi pola aktivitas anomali pada data log berskala besar serta meningkatkan keamanan sistem melalui autentikasi dua faktor (OTP Telegram) dan notifikasi otomatis. Sistem ini dapat dikembangkan lebih lanjut dengan menambah variasi data log nyata dan menerapkan metode pembelajaran mendalam untuk meningkatkan akurasi deteksi.*

1. PENDAHULUAN

Keamanan website merupakan aspek krusial dalam menjaga integritas dan ketersediaan layanan digital di era modern. Meningkatnya aktivitas daring dan transaksi berbasis web membuat sistem semakin rentan terhadap berbagai bentuk serangan siber seperti brute force attack, SQL injection, maupun akses ilegal yang memanfaatkan celah keamanan aplikasi [1]. Serangan-serangan tersebut tidak hanya menyebabkan kerugian finansial, tetapi juga dapat mengancam reputasi institusi dan kepercayaan pengguna terhadap system [2]. Oleh karena itu, dibutuhkan pendekatan keamanan yang mampu mendeteksi dan menganalisis aktivitas mencurigakan secara cepat dan akurat.

Salah satu pendekatan yang efektif dalam meningkatkan keamanan website adalah melalui analisis log aktivitas jaringan. Log berfungsi sebagai sumber data utama yang mencatat seluruh interaksi antara pengguna dan sistem, sehingga dapat digunakan untuk mengidentifikasi pola aktivitas yang menyimpang dari perilaku normal. Namun, proses analisis log secara manual dinilai tidak efisien karena volume data yang sangat besar dan terus meningkat. Untuk mengatasi hal tersebut, pendekatan statistik dapat diterapkan guna mengenali pola anomali berdasarkan distribusi data dan frekuensi kejadian tertentu,

sehingga sistem mampu mendeteksi potensi ancaman secara otomatis [3].

Dalam penelitian ini, dikembangkan sebuah sistem keamanan bernama SecurityShield, yang dirancang untuk mendeteksi aktivitas anomali pada website melalui analisis log dan metode statistik. Sistem ini dilengkapi dengan database anomalies yang berfungsi mencatat seluruh aktivitas mencurigakan seperti alamat IP sumber, waktu kejadian, dan jenis anomali yang terdeteksi. Data tersebut kemudian dianalisis secara statistik untuk menentukan tingkat risiko dan mempermudah administrator dalam mengambil keputusan preventif terhadap potensi serangan [4].

Selain aspek deteksi, sistem SecurityShield juga mengutamakan kemudahan dalam pemantauan keamanan melalui antarmuka pengguna yang interaktif. Tampilan dashboard dirancang untuk menampilkan informasi penting seperti jumlah log aktivitas, tingkat ancaman, serta grafik visual anomali secara real-time. Desain ini tidak hanya mempermudah proses analisis, tetapi juga meningkatkan efisiensi pengawasan keamanan oleh administrator jaringan [5].

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada implementasi sistem keamanan website berbasis analisis log dan deteksi aktivitas anomali menggunakan pendekatan statistik. Sistem yang dikembangkan diharapkan dapat menjadi solusi efektif dalam meningkatkan deteksi dini terhadap ancaman siber serta memberikan visualisasi data keamanan yang informatif dan mudah diinterpretasikan.

Ditambah dengan penelitian yang dilakukan [6] dimana hasil yang didapat adalah Penelitian ini menunjukkan bahwa model Isolation Forest berhasil mendeteksi 499 anomali (5%) dari 10.041 log web server Apache, terutama pada ukuran respons dan status error 404. Dengan mean score -0.3802 dan standar deviasi 0.0023, model terbukti konsisten dan efektif. Hasil ini menegaskan bahwa Isolation Forest dapat digunakan sebagai metode andal untuk deteksi anomali dan pemantauan keamanan web server secara real-time.

2. TINJAUAN PUSTAKA

Penelitian ini berfokus pada penerapan pendekatan statistik dan pembelajaran mesin (Machine Learning) untuk meningkatkan kemampuan sistem dalam mendeteksi aktivitas anomali pada website secara otomatis. Empat aspek utama yang mendukung penelitian ini meliputi logging system sebagai sumber data aktivitas, WebSocket untuk komunikasi real-time, algoritma Isolation Forest dalam mendeteksi anomali, serta penerapan keamanan web melalui autentikasi, enkripsi, dan verifikasi. Keempat komponen tersebut saling terintegrasi guna membangun sistem keamanan yang adaptif, responsif, dan andal [7].

2.1. Konsep Logging System

Logging system merupakan sistem yang digunakan untuk merekam setiap aktivitas atau peristiwa yang terjadi pada suatu sistem, baik dalam bentuk error, request, maupun response dari pengguna. Tujuan utama logging adalah untuk melakukan monitoring, debugging, dan analisis keamanan terhadap suatu sistem. Setiap log yang dikumpulkan dapat membantu administrator dalam mendeteksi anomali, mengidentifikasi serangan, serta memulihkan sistem dari kesalahan.

Logging system yang baik harus memiliki komponen real-time log collection, centralized storage, dan analisis otomatis agar proses deteksi insiden menjadi lebih cepat. Logging yang dilakukan secara terdistribusi dan tersentralisasi juga mampu meningkatkan efisiensi dalam mengelola ribuan event dari berbagai sumber data [8].

2.2. WebSocket untuk Komunikasi Real-Time

WebSocket merupakan protokol komunikasi dua arah (full-duplex) antara klien dan server melalui satu koneksi TCP tunggal. Dengan WebSocket, data dapat dikirim dan diterima secara real-time tanpa perlu melakukan request berulang (polling) seperti pada HTTP konvensional.

Oleh karena itu, penggunaan WebSocket memungkinkan sistem berbasis web untuk mengirim notifikasi instan, seperti peringatan keamanan atau log baru yang muncul tanpa perlu refresh halaman. Hal ini sangat berguna dalam sistem monitoring atau logging [9].

2.3. Machine Learning dan Isolation Forest

Machine Learning (ML) merupakan cabang dari kecerdasan buatan (AI) yang

memungkinkan sistem untuk belajar dari data dan membuat keputusan tanpa pemrograman eksplisit. Salah satu algoritma yang populer untuk mendeteksi anomali adalah Isolation Forest (iForest).

Isolation Forest bekerja dengan prinsip isolation, yaitu memisahkan data outlier dari data normal dengan membangun random decision trees. Data yang mudah diisolasi cenderung merupakan anomali. Untuk mengatasi hal tersebut, metode ini efisien untuk data berskala besar karena memiliki kompleksitas waktu yang rendah [10].

2.4. Dasar Keamanan Web (Session, Autentikasi, OTP Telegram, Enkripsi, dan Verifikasi)

Keamanan web merupakan aspek penting dalam pengembangan sistem berbasis web. Aspek utama yang harus diperhatikan meliputi session management, autentikasi, One-Time Password (OTP), enkripsi data, dan verifikasi pengguna. Session management digunakan untuk menyimpan status pengguna selama interaksi dengan sistem. Autentikasi memastikan bahwa pengguna yang mengakses sistem adalah pihak yang sah. OTP Telegram menjadi metode verifikasi tambahan berbasis notifikasi real-time melalui bot Telegram yang lebih praktis dan cepat. Enkripsi data menjaga kerahasiaan informasi sensitif dari serangan man-in-the-middle. Verifikasi dua langkah (2FA) memberikan lapisan keamanan ekstra terhadap akun pengguna.

Kombinasi OTP Telegram dan autentikasi berbasis token JWT mampu mengurangi risiko unauthorized access pada aplikasi berbasis web [11].

3. METODE PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini merupakan penelitian eksperimen dan pengembangan sistem (R&D) untuk mengembangkan sistem dan menyempurnakan sistem yang telah ada dan digunakan untuk menguji ke efektifan sistem tersebut [12]. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan website berbasis analisis log dan deteksi aktivitas anomali secara real-time. Pendekatan yang digunakan adalah pendekatan kuantitatif dengan analisis data log menggunakan algoritma machine learning Isolation Forest untuk mendeteksi aktivitas tidak normal (anomali).

3.2. Desain Sistem

Sistem keamanan website yang dikembangkan pada penelitian ini dirancang dalam bentuk arsitektur tiga komponen terintegrasi yang saling berinteraksi, yaitu:

3.2.1. Sistem Logging dan Autentikasi

Komponen pertama sistem ini berfungsi sebagai dasar keamanan dengan memastikan proses autentikasi dan pencatatan aktivitas pengguna berlangsung menyeluruh. Setiap interaksi seperti login, logout, registrasi, dan aktivitas lain dicatat lengkap dengan timestamp, alamat IP, user agent, dan jenis aksi. Sistem ini juga menerapkan autentikasi dua faktor (2FA) melalui Telegram Bot API, di mana pengguna harus memverifikasi kode OTP yang dikirim secara real-time untuk mencegah akses ilegal. Selain itu, keamanan data dijaga menggunakan algoritma bcrypt dengan fungsi password_hash() pada PHP, sehingga password terenkripsi dan tidak dapat dikembalikan ke bentuk aslinya meskipun terjadi pelanggaran sistem [13].

3.2.2. Deteksi Anomali

Komponen kedua berfokus pada deteksi anomali. Deteksi anomali adalah proses mencari data dengan perilaku yang berbeda dari biasanya [14]. Deteksi nya menggunakan algoritma Isolation Forest. Sistem ini memantau tiga parameter utama, yaitu Request Rate Analysis untuk mendeteksi lonjakan permintaan dari suatu IP, Brute-Force Detection untuk mengenali login gagal berulang dalam waktu singkat, dan Temporal Anomaly Detection untuk mengidentifikasi aktivitas di luar jam operasional normal.

3.2.3 Dashboard Admin

Dashboard Admin berfungsi sebagai pusat pemantauan utama yang menampilkan seluruh aktivitas pengguna dan log sistem secara real-time melalui koneksi WebSocket. Dimana cara kerja websocket yaitu menyimpan state atau koneksi pengguna di server yang membuat server memerlukan banyak aplikasi untuk menyimpan koneksi tersebut [15]. Dashboard ini dilengkapi dengan fitur visualisasi interaktif, seperti grafik aktivitas log per jam untuk

memantau intensitas penggunaan sistem, serta grafik jumlah anomali per hari yang membantu mendeteksi pola serangan atau aktivitas mencurigakan.

Selain itu, admin dapat mengekspor data log ke format Excel (XLSX) atau CSV untuk keperluan analisis lanjutan atau pelaporan. Sistem juga memiliki fitur notifikasi otomatis yang memberikan peringatan "High Risk" ketika jumlah anomali melebihi ambang batas tertentu, sehingga admin dapat segera mengambil tindakan terhadap potensi ancaman keamanan.

3.3. Alur Penelitian

3.3.1. Perancangan sistem

Rancangan yang dibangun mencakup arsitektur hubungan antara logging, autentikasi (login, registrasi, OTP Telegram), database MySQL, dan deteksi anomali. Dan juga perancangan struktur tabel di database, seperti tabel users, logs, dan anomalies, yang berfungsi untuk menyimpan data aktivitas pengguna secara sistematis.

3.3.2 Pembuatan dataset

Dataset simulasi log dibuat melalui skrip yang meniru aktivitas pengguna secara realistis, mencakup perilaku normal dan anomali seperti brute-force login, flood request, serta login di luar jam kerja. Data hasil simulasi ini digunakan untuk melatih model Isolation Forest agar mampu membedakan aktivitas normal dan mencurigakan. Proses dijalankan secara dinamis melalui Command Line (CMD) untuk menghasilkan log secara real-time.

3.3.3 Integrasi Isolation Forest

Proses deteksi anomali, di mulai dengan menerapkan pendekatan machine learning menggunakan algoritma Isolation Forest. Model ini dilatih dengan menggunakan dataset simulasi log yang sebelumnya telah dibuat, berisi kombinasi aktivitas normal dan aktivitas anomali. Selama proses pelatihan, algoritma membangun sejumlah isolation trees untuk mempelajari pola distribusi data dan menghitung anomaly score bagi setiap aktivitas pengguna.

Sebelum data log digunakan untuk dianalisis oleh model Isolation Forest, maka harus mellaui pre-processing yang meliputi pembersihan data duplikat atau kosong, normalisasi format seperti waktu dan status login, serta ekstraksi fitur penting seperti jam login, jumlah login gagal, frekuensi permintaan, dan akses ke endpoint sensitif. Selain itu, sistem juga menerapkan rule-based pre-scoring untuk memberi nilai risiko awal sebelum data diproses oleh model.

Cara kerja Isolation Forest dimulai dengan membuat beberapa pohon keputusan secara acak. Setiap pohon dibangun dengan memilih fitur secara acak dan kemudian membagi data berdasarkan nilai acak dari fitur tersebut. Proses ini berulang hingga setiap sampel data benar-benar terisolasi dalam sebuah node. Kedalaman rata-rata di mana suatu sampel terisolasi di semua pohon digunakan untuk menghitung skor anomali. Semakin cepat sebuah sampel terisolasi (yaitu, semakin rendah kedalamannya), semakin besar kemungkinan bahwa sampel tersebut adalah anomali. Secara matematis, skor anomali untuk sebuah sampel x dapat dihitung sebagai:

$$S(x, n) = 2^{\frac{E(h(x))}{c(n)}} \quad (1)$$

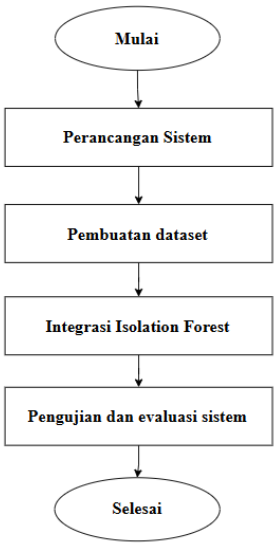
dimana :

- E(h(x)) adalah kedalaman rat a-rata dari sampel x di semua pohon dalam hutan.
- c(n) adalah fungsi yang mendekati kedalaman rata-rata untuk pohon yang sepenuhnya dibangun dan digunakan untuk normalisasi. Nilai skor ini berada pada rentang [-1, 1], dengan nilai mendekati -1 menunjukkan kemungkinan besar anomali [6].

3.3.4 Pengujian dan evaluasi sistem

Pengujian dan evaluasi sistem dilakukan untuk menilai sejauh mana model deteksi anomali mampu mengenali aktivitas mencurigakan secara akurat dan efisien. Proses pengujian mencakup analisis metrik performa seperti precision, recall, F1 score, dan accuracy untuk mengukur ketepatan serta kemampuan model dalam mendeteksi anomali.

Selain itu, analisis feature importance digunakan untuk mengetahui faktor yang paling memengaruhi hasil deteksi, seperti waktu login, jumlah percobaan login gagal, dan frekuensi akses ke endpoint sensitif. Melalui hasil pengujian ini, dapat disimpulkan bahwa sistem sudah mampu melakukan deteksi awal terhadap aktivitas berisiko, namun masih perlu penyempurnaan agar dapat meningkatkan tingkat sensitivitas dan akurasi secara keseluruhan.



Gambar 1. Flowchart alur Penelitian

3.4. Arsitektur Website

3.4.1 Interaksi User

Tahapan ini merupakan titik awal di mana pengguna melakukan aktivitas seperti login atau registrasi melalui antarmuka website. Setiap tindakan pengguna akan secara otomatis dikirim ke server dalam bentuk data aktivitas (event) yang berisi informasi seperti username, timestamp, IP address, dan jenis aksi (misalnya login, logout, atau registrasi). Dimana untuk login baik admin maupun user menggunakan authentikasi berupa toke OTP yang dikirim ke bot telegram.

3.4.2 Logging System (Sistem Pencatatan Aktivitas)

Setelah data aktivitas diterima oleh server, sistem akan mencatatnya ke dalam database MySQL pada tabel log. Setiap entri log memuat detail lengkap seperti waktu kejadian, alamat IP, jenis perangkat (user agent), dan status aktivitas (berhasil/gagal). Komponen ini menjadi sumber utama bagi analisis selanjutnya karena menyimpan seluruh jejak aktivitas pengguna di dalam sistem.

3.4.3 Deteksi Anomali - Isolation Forest

Data log terbaru yang masuk akan diproses oleh model Machine Learning Isolation Forest untuk menghitung nilai anomaly score yaitu ukuran seberapa jauh suatu aktivitas menyimpang dari perilaku normal pengguna. Jika skor tersebut melewati threshold (ambang batas), maka aktivitas tersebut akan dikategorikan sebagai anomali. Dimana Isolation Forest ini belajar dari dataset yang telah di buat.

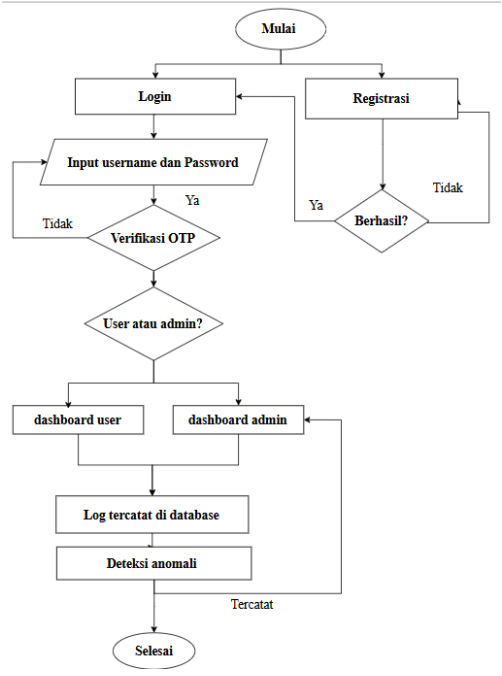
3.4.4 WebSocket Real-time Monitoring

Untuk memastikan sistem dapat merespons ancaman secara cepat, hasil analisis dari modul deteksi anomali dikirim langsung ke dashboard admin melalui WebSocket. Teknologi ini memungkinkan pembaruan data secara real-time tanpa perlu refresh halaman, sehingga admin dapat langsung melihat aktivitas mencurigakan begitu terjadi.

3.4.5 Dashboard Admin dan user

Bagian ini menjadi pusat kontrol bagi administrator. Dashboard menampilkan grafik aktivitas log per jam, jumlah anomali harian, dan notifikasi risiko tinggi (High Risk Alert) jika aktivitas anomali melebihi ambang batas tertentu. Selain itu, admin dapat mengekspor data log ke format Excel (XLSX) atau CSV untuk keperluan analisis lanjutan atau pelaporan.

Untuk dashboard user hanya dapat melihat aktivitas user, login, terakhir login dan informasi website lainnya.



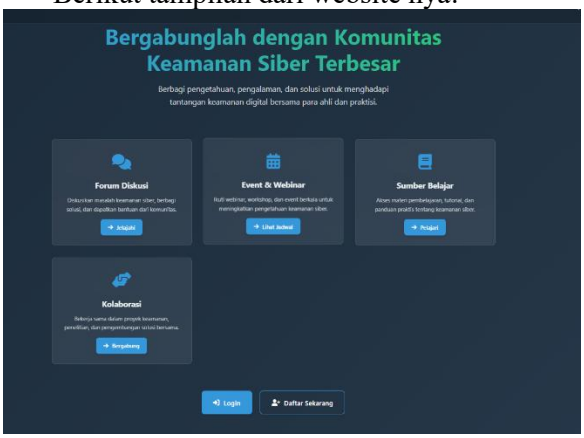
Gambar 2. Flowchart arsitektur Website

4. HASIL DAN PEMBAHASAN

Hasil implementasi sistem menunjukkan bahwa platform Sistem Logging dan Deteksi

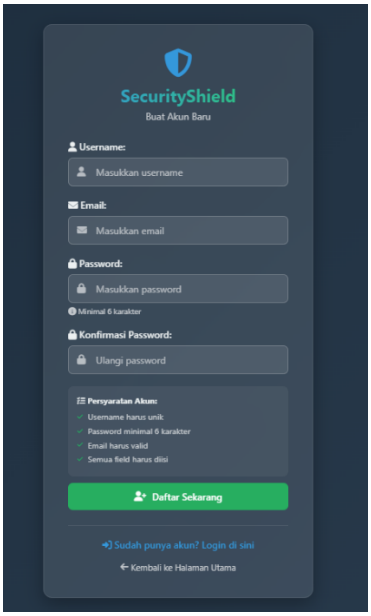
Anomali Berbasis Website berhasil berjalan sesuai rancangan. Sistem ini mampu mencatat seluruh aktivitas pengguna baik admin maupun user secara real-time, mulai dari proses login, logout, hingga registrasi, lengkap dengan informasi timestamp, IP address, user agent, dan status aktivitas. Autentikasi login juga berhasil dikombinasikan dengan OTP Telegram, di mana pengguna wajib memasukkan kode verifikasi yang dikirim langsung ke akun Telegram mereka sebelum dapat mengakses dashboard.

Berikut tampilan dari website nya:



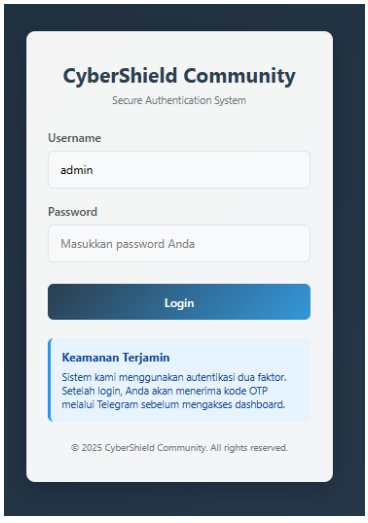
Gambae 3. Halaman home website

Gambar 3 ini merupakan Halaman home yang berfungsi sebagai portal utama bagi pengguna untuk mengakses berbagai fitur keamanan siber seperti forum diskusi, event & webinar, sumber belajar, dan kolaborasi. Melalui halaman ini, pengguna dapat melakukan login atau registrasi menggunakan autentikasi OTP yang dikirim ke Telegram, sehingga keamanan akses lebih terjamin. Setiap aktivitas login atau registrasi otomatis tercatat dalam sistem logging yang kemudian dianalisis oleh model Isolation Forest untuk mendeteksi potensi anomali. Tampilan dashboard yang interaktif juga menampilkan informasi aktivitas komunitas seperti jumlah anggota, event, dan diskusi aktif, menjadikannya tidak hanya sebagai gerbang masuk ke sistem deteksi anomali tetapi juga sebagai pusat interaksi dan edukasi bagi seluruh pengguna.



Gambar 4. Halaman registrasi

Gambar 4 merupakan halaman yan g digunakan untuk membuat akun baru dengan mengisi data seperti username, email, dan password. Setelah menekan tombol “Daftar Sekarang”, data dikirim ke server, disimpan dalam database MySQL, dan pengguna menerima kode OTP melalui Telegram untuk verifikasi. Aktivitas registrasi ini otomatis tercatat dalam sistem log dan dipantau oleh modul Isolation Forest untuk mendeteksi anomali secara real-time.



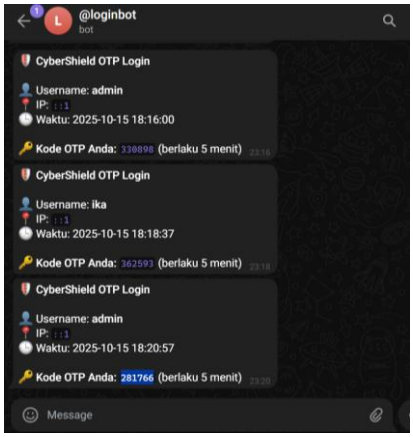
Gambar 5. Halaman login

Gambar 5 merupakan halaman login yang berfungsi sebagai gerbang utama autentikasi pengguna. Pada halaman ini, pengguna harus memasukkan username dan password untuk memverifikasi identitasnya. Setelah menekan

tombol “Login”, sistem akan mengirimkan kode OTP ke akun Telegram pengguna sebagai bagian dari proses autentikasi dua faktor (Two-Factor Authentication) untuk memastikan keamanan tambahan sebelum mengakses dashboard. Informasi login seperti waktu, IP address, dan status autentikasi (berhasil/gagal) secara otomatis dicatat ke dalam sistem log MySQL, kemudian dipantau oleh modul Isolation Forest untuk mendeteksi potensi aktivitas anomali secara real-time.

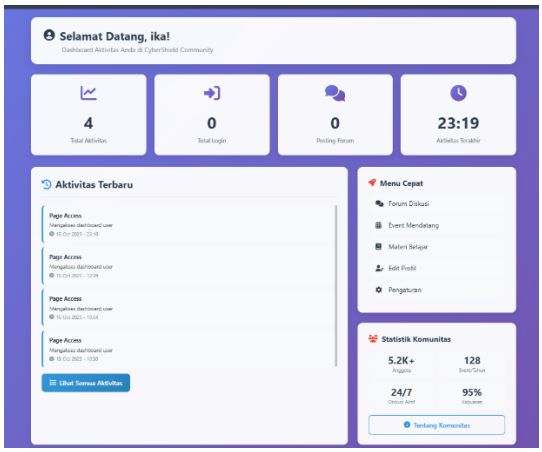
Gambar 6. Halaman Verifikasi OTP

Gambar 6 merupakan halaman yang berfungsi sebagai tahap kedua dalam proses autentikasi dua faktor (Two-Factor Authentication). Setelah pengguna berhasil login menggunakan username dan password, sistem secara otomatis mengirimkan kode OTP ke akun Telegram pengguna melalui bot resmi CyberShield. Pengguna kemudian harus memasukkan kode tersebut ke kolom verifikasi sebelum waktu hitung mundur berakhir (misalnya 5 menit). Jika OTP yang dimasukkan benar, pengguna diarahkan ke dashboard sesuai rolenya (admin atau user). Seluruh aktivitas verifikasi, baik yang berhasil maupun gagal, akan dicatat ke dalam sistem log MySQL untuk dianalisis lebih lanjut oleh modul deteksi anomali Isolation Forest, yang bertugas mengidentifikasi potensi percobaan login mencurigakan secara real-time.



Gambar 7 OTP masuk ke Bot Telegram

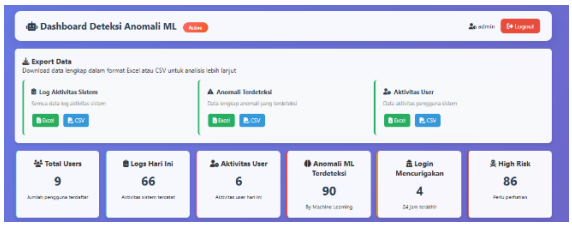
Gambar 7 menunjukkan notifikasi kode OTP login dari bot Telegram CyberShield OTP Login yang dikirim setiap kali pengguna melakukan login ke sistem. Pesan berisi username, alamat IP, waktu login, dan kode OTP yang berlaku selama 5 menit sebagai verifikasi dua faktor (2FA). Sistem ini meningkatkan keamanan login, mencatat aktivitas ke database MySQL, dan menganalisisnya dengan algoritma Isolation Forest untuk mendeteksi anomali login secara real-time.



Gambar 8. Halaman dashboard User

Gambar 8 ini merupakan halaman untuk user yang dimana user dapat melihat statistik singkat seperti total aktivitas, jumlah login, posting forum, dan waktu aktivitas terakhir. Bagian tengah menampilkan daftar aktivitas terbaru yang mencatat halaman-halaman yang baru diakses pengguna. Dan juga informasi singkat tentang website ini berupa menu cepat untuk menuju ke forum diskusi, event mendatang, materi belajar, edit profil, dan pengaturan. Selain itu, ada juga statistik komunitas yang menampilkan jumlah anggota, pengajar, akses

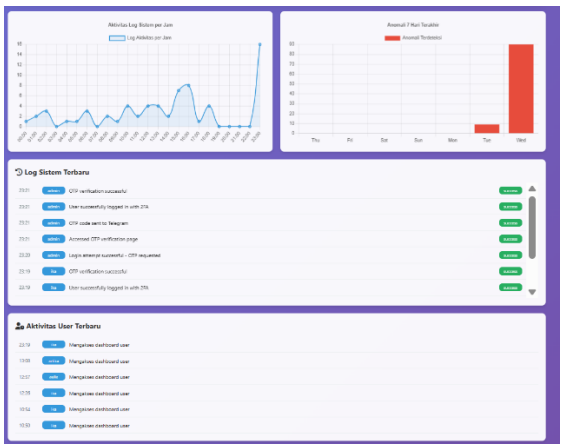
24 jam, serta tingkat partisipasi. Secara keseluruhan, dashboard ini memberikan gambaran ringkas mengenai aktivitas pengguna sekaligus informasi umum tentang komunitas.



Gambar 9 Halaman dashboard admin

Gambar 9 merupakan dashboard admin sistem deteksi anomali berbasis Machine Learning (ML) yang digunakan untuk memantau aktivitas pengguna dan mendeteksi perilaku mencurigakan dalam sistem. Pada bagian atas terdapat judul "Dashboard Deteksi Anomali ML" dengan status Active yang menandakan sistem sedang berjalan, serta tampilan nama admin dan tombol logout di sisi kanan. Bagian Export Data menyediakan tiga jenis data yang dapat diunduh, yaitu log aktivitas sistem, data anomali yang terdeteksi, dan aktivitas pengguna, masing-masing dalam format Excel atau CSV untuk analisis lebih lanjut.

Di bawahnya, terdapat rangkuman statistik penting seperti jumlah total pengguna, jumlah login hari ini, aktivitas pengguna, anomali yang terdeteksi oleh model ML, login mencurigakan, serta aktivitas berisiko tinggi (High Risk). Secara keseluruhan, dashboard ini berfungsi sebagai pusat kontrol bagi admin untuk melakukan pengawasan keamanan, menganalisis anomali, dan menjaga stabilitas sistem secara efisien.



Gambar 10. statistik logs dan deteksi anomali

Pada gambar 10 menunjukkan dashboard pemantauan aktivitas sistem dan pengguna dalam sistem deteksi anomali. Pada bagian atas terdapat dua grafik yang menampilkan aktivitas log sistem per jam dan jumlah anomali yang terdeteksi per hari, di mana grafik menunjukkan peningkatan aktivitas dan anomali pada waktu tertentu.

Di bawahnya terdapat tabel Log Sistem Terbaru yang mencatat detail aktivitas sistem seperti autentikasi OTP, login berhasil, dan permintaan verifikasi lengkap dengan waktu dan statusnya. Sementara itu, bagian Aktivitas User Terbaru menampilkan aktivitas pengguna seperti login, logout, dan akses ke halaman dashboard. Secara keseluruhan, dashboard ini berfungsi untuk memantau aktivitas sistem dan perilaku pengguna secara real-time guna mendeteksi anomali serta menjaga keamanan sistem

Gambar 11. Evaluasi model Isolation Forest

Gambar tersebut menampilkan hasil evaluasi model deteksi anomali berbasis Machine Learning (ML) yang menunjukkan performa model melalui beberapa metrik utama dan analisis fitur. Nilai precision sebesar 80% menunjukkan bahwa sebagian besar prediksi anomali benar, namun recall hanya 8,7% menandakan model masih melewatkan banyak anomali. F1 score sebesar 15,7% menggambarkan keseimbangan yang rendah antara ketepatan dan cakupan deteksi, sementara accuracy 57% menunjukkan akurasi keseluruhan yang masih sedang.

Pada bagian feature importance, faktor yang paling berpengaruh terhadap deteksi adalah waktu login, percobaan login gagal, akses ke endpoint sensitif, frekuensi permintaan, dan risiko lokasi pengguna. Bagian bawah menunjukkan hasil confusion matrix, dengan 4 anomali terdeteksi benar (true positive), 1 deteksi salah (false positive), 53 aktivitas normal benar (true negative), dan 42 anomali yang tidak terdeteksi (false negative). Secara

keseluruhan, model memiliki ketepatan tinggi namun sensitivitas rendah, sehingga masih perlu peningkatan dalam mendeteksi lebih banyak anomali secara akurat.

5. KESIMPULAN

Berdasarkan hasil penelitian, sistem keamanan website berbasis analisis log dan algoritma Isolation Forest berhasil diimplementasikan dengan baik untuk mendeteksi aktivitas anomali secara real-time. Sistem ini mampu mencatat seluruh aktivitas pengguna, melaksanakan autentikasi dua faktor melalui OTP Telegram, serta menampilkan hasil deteksi anomali pada dashboard interaktif yang terhubung menggunakan WebSocket. Hasil pengujian menunjukkan bahwa model memiliki nilai precision sebesar 80%, recall sebesar 8,7%, F1-score sebesar 15,7%, dan akurasi 57%. Hal ini menandakan bahwa sistem memiliki tingkat ketepatan yang cukup tinggi, meskipun masih terbatas dalam mendeteksi seluruh aktivitas anomali secara menyeluruh.

Kelebihan sistem ini terletak pada kemampuannya bekerja secara real-time dengan notifikasi otomatis melalui Telegram Bot API, serta penggunaan algoritma Isolation Forest yang efektif dalam mengenali pola aktivitas tidak normal dari data log berskala besar. Selain itu, dashboard admin yang interaktif dan informatif sangat membantu dalam proses pemantauan keamanan, sementara autentikasi dua faktor meningkatkan perlindungan terhadap akses ilegal.

Namun demikian, sistem masih memiliki beberapa kekurangan, antara lain nilai recall yang rendah sehingga model belum mampu mendeteksi semua anomali dengan optimal, serta keterbatasan data pelatihan yang masih bersifat simulasi sehingga mengurangi kemampuan generalisasi model terhadap kondisi nyata. Selain itu, sistem belum memiliki mekanisme otomatis untuk menyesuaikan parameter atau beradaptasi terhadap pola serangan baru.

Untuk pengembangan selanjutnya, sistem dapat disempurnakan dengan menambah variasi dan volume data log nyata guna meningkatkan akurasi model. Penggunaan metode ensemble learning atau deep learning seperti Autoencoder dan LSTM juga dapat menjadi alternatif untuk mendeteksi anomali yang lebih kompleks. Selain itu, integrasi sistem pembelajaran mandiri (self-learning system) serta pengembangan notifikasi berbasis perangkat seluler dan laporan otomatis diharapkan dapat meningkatkan efektivitas dan kecepatan respons terhadap ancaman keamanan di masa mendatang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dalam penyelesaian penelitian ini. Terima kasih disampaikan kepada dosen pembimbing dan rekan-rekan di lingkungan akademik yang telah memberikan masukan, saran, serta motivasi selama proses perancangan dan pengujian sistem keamanan website berbasis analisis log dan deteksi aktivitas anomali menggunakan algoritma Isolation Forest.

Ucapan terima kasih juga ditujukan kepada institusi yang telah menyediakan fasilitas penelitian serta lingkungan yang kondusif untuk pengembangan sistem ini. Tanpa dukungan moral, teknis, dan akademik dari berbagai pihak, penelitian ini tidak akan terselesaikan dengan baik.

DAFTAR PUSTAKA

[1] N. A, W. J And C. K, “Comprehensive Analysis And Evaluation Of Anomalous User Activity In Web Server Logs,” Sensors, Vol. Vol.24, No. No.3, Pp. 1-15, 2024.

[2] R. A.-B. R And A.-A. M, “Web Traffic Anomaly Detection Using Isolation Forest,” Informatics, Vol. Vol.11, No. No.4, Pp. 1-12, 2024.

[3] K. S. Y And K. T, “Impact Of Log Parsing On Deep Learning-Based Anomaly Detection,” Empirical Software Engineering, Vol. Vol.29, No. No.2, Pp. 1-20, 2024.

[4] H. R. M, L. K And P. S, “Enhanced Web Server Log Anomaly Detection Using Hybrid Clustering And Machine Learning For Time Series Data,” Journal Of Information Science And Information Security (Jisis), Vol. Vol.21, No. No.1, Pp. 33-48, 2025.

[5] A. F. D And Y. R, “A Siem-Driven Solution For Cyber Attack Detection In Educational Websites: Implementing Threat Log Filtering For Enhanced Security,” Jupiter: Jurnal Penelitian Ilmu Dan Teknologi Komputer, Vol. Vol.6, No. No.1, Pp. 45-53, 2025.

[6] D. B. Santoso And Y. Wahyuni, “Web Server Log System As An Anomaly Detector Using

Isolation Forest," Jurnal Aplikasi Bisnis Dan Komputer (Jubikom), Vol. Vol.4, No. No.3, Pp. 90-96, 2024.

[7] H. P. N, S. S. A And I. R. M, "Analisis Log Server Untuk Mendeteksi Serangan Ddos Pada Keamanan Jaringan Di Website," Pjiset: Public Journal Of Information System And Emerging Technology, Vol. Vol.3, No. No.2, Pp. 77-85, 2025.

[8] P. A, S. S, M. L, S. A, P. D, T. P And S. T, "Centralized It Logging System," International Journal Of Advanced Research In Computer And Communication Engineering (Ijarcce), Vol. Vol.13, No. No.4, Pp. 45-50, 2024.

[9] P. B And G. P, "Enhancing Real-Time Web Applications With Websockets: Performance And Responsiveness," International Journal Of Novel Research And Development (Ijnrd), Vol. Vol.9, No. No.6, Pp. 120-126, 2024.

[10] A. S And A. M, "Web Traffic Anomaly Detection Using Isolation Forest," Informatics, Vol. Vol.11, No. No.4, Pp. 1-15, 2023.

[11] P. S. P, N. P. A And R. H. M, "Door Security System Using E-Ktp And One Time Password (Otp) Code With Telegram Messenger Notification," Indonesian Journal Of Electrical And Electronics Engineering (Inajeee), Vol. Vol.2, No. No.1, Pp. 15-22, 2024.

[12] A. Rustamana, K. H. Sahl, D. Ardianti And A. H. Syauqi, "Penelitian Dan Pengembangan (Research & Development) Dalam Pendidikan," Jurnal Bima: Pusat Publikasi Ilmu Pendidikan Bahasa Dan Sastra, Vol. Vol.2, No. No.3, Pp. 60-69, 2024.

[13] K. N. Isnaini, D. Suhartono, M. T. Jamil And A. Qothrunnada, "Implementasi Pengamanan Data Menggunakan Teknik Bcrypt Hashing Password Dan Algoritma Advanced Encryption Standard (Aes)," Jurnal Sistem Dan Teknologi Informasi (Justin), Vol. Vol.13, No. No.1, Pp. 101-108, 2025.

[14] D. R. K. Saputra, Y. V. Via And A. N. Sihananto, "Deteksi Anomali Menggunakan Ensemble Learning Dan Random Over Sampling Pada Penipuan Transaksi Keuangan," Jitet (Jurnal Informatika Dan Teknik Elektro Terapan), Vol. Vol.12, No. No.3, Pp. 2779-2788, 2024.

[15] R. M. Rishwan, E. H. Nurkifli And A. Solehudin, "Analisis Perbandingan Performa Server Websocket Dengan Menggunakan Payload Json, Binary Serialization, Dan Protobuf Dengan Menggunakan Metode Load Testing," Jurnal Mahasiswa Teknik Informatika (Jati), Vol. Vol.9, No. No.1, Pp. 706-712, 2025.