DETEKSI SERANGAN *PASSWORD SPRAYING* SECARA *REALTIME* MENGGUNAKAN ALGORITMA ISOLATION FOREST BERDASARKAN ANALISIS FITUR *LOG* AUTENTIKASI

SKRIPSI

Karya tulis sebagai salah satu syarat
untuk memperoleh gelar Sarjana
dari Universitas Indo Global Mandiri

Oleh
M.ROBY
NPM: 2022310034
SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDO GLOBAL MANDIRI
2026

DETEKSI SERANGAN PASSWORD SPRAYING SECARA REALTIME MENGGUNAKAN ALGORITMA ISOLATION FOREST BERDASARKAN ANALISIS FITUR LOG AUTENTIKASI

HALAMAN PENGESAHAN

Oleh

M.ROBY
2022310034
Program Studi Sarjana Sistem Komputer

Universitas Indo Global Mandiri

Menyetujui
Tim Pembimbing

Tanggal, 30 Juli 2026

Pembimbing 1	Pembimbing 2
Ferdiansyah, M.Kom., Ph.D., CEH	Tasmi, S.Si., M.Kom.
2024.01.03.75	2017.01.02.30

Mengetahui,
Dekan Fakultas Ilmu Komputer & Sains

FAKULTAS ILKOM & SAINS
UIGM

Dr. Herri Setiawan, S.Kom., M.Kom.
2003.01.00.60

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari ini Senin Tanggal 30 Juli 2026 telah dilaksanakan Ujian Skripsi oleh Program Studi Sistem Komputer Fakultas Ilmu Komputer & Sains Universitas Indo Global Mandiri Palembang.

Menyetujui
Tim Penguji

Palembang, 30 Juli 2026

Ketua Penguji

Ferdiansyah, M.Kom., Ph.D., CEH
2024.01.03.75

Penguji 1

Ricky Maulana Fajri, S.Kom., M.Sc., Ph.D.
2016.01.02.20

Penguji 2

Candra Setiawan, S.T., M.T
2016.01.00.31

Mengetahui
Ketua Program Studi Sistem Komputer

Tasmi, S.Si., M.Kom.
2017.01.02.30

SURAT KETERANGAN REVISI SKRIPSI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa:

Nama : M.ROBY

NPM : 2022310034

Judul Skripsi : DETEKSI SERANGAN PASSWORD SPRAYING SECARA REALTIME MENGGUNAKAN ALGORITMA ISOLATION FOREST BERDASARKAN ANALISIS FITUR LOG AUTENTIKASI.

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan skripsi.

Menyetujui
Tim Penguji

Palembang, 3 Agustus 2026

Ketua Penguji

Ferdiansyah, M.Kom., Ph.D., CEH
2024.01.03.75

Penguji 1

Ricky Maulana Fajri, S.Kom., M.Sc., Ph.D.
2016.01.02.20

Penguji 2

Candra Setiawan, S.T., M.T
2016.01.00.31

Mengetahui
Ketua Program Studi Sistem Komputer

Tasmi, S.Si., M.Kom.
2017.01.02.30

ABSTRAK

DETEKSI SERANGAN *PASSWORD SPRAYING* SECARA *REALTIME* MENGGUNAKAN ALGORITMA ISOLATION FOREST BERDASARKAN ANALISIS FITUR *LOG* AUTENTIKASI

Serangan *Password Spraying* merupakan ancaman keamanan yang sulit dideteksi karena pelaku mencoba sejumlah kecil kata sandi umum terhadap banyak akun, sehingga aktivitasnya menyerupai kegagalan *log*in yang wajar dan tidak memicu mekanisme penguncian akun. Permasalahan yang dikaji dalam penelitian ini adalah bagaimana membangun sistem yang dapat mencatat aktivitas autentikasi dan mendeteksi serangan *Password Spraying* secara *realtime*. Penelitian ini bertujuan membangun sistem pencatatan aktivitas autentikasi dan mengimplementasikan algoritma Isolation Forest untuk mendeteksi serangan tersebut berdasarkan analisis fitur *log* autentikasi. Tahapan penelitian meliputi perancangan sistem *log*ging, pelabelan data berdasarkan pengelompokan aktivitas dalam jendela waktu satu menit, serta pelatihan model menggunakan pendekatan *semi-supervised*, yaitu model dilatih hanya pada data berlabel normal. Pengujian dilakukan pada *dataset* hasil simulasi sebanyak 4.213 record dengan tiga skenario pembagian data latih dan uji, yaitu 70:30, 80:20, dan 90:10. Pada skenario 80:20, model memperoleh akurasi 96,44%, ROC-AUC 0,9581, dan *recall* 1,00 pada kelas serangan, yang berarti seluruh serangan *Password Spraying* pada data uji terdeteksi tanpa ada yang terlewat. Dengan demikian, dapat disimpulkan bahwa algoritma Isolation Forest dapat diterapkan untuk mendeteksi serangan *Password Spraying* secara *realtime* berdasarkan fitur *log* autentikasi.

Kata kunci: *Password Spraying*, Isolation Forest, *log* autentikasi, *semi-supervised*, *realtime*

ABSTRACT

DETECTION OF REALTIME PASSWORD SPRAYING ATTACKS USING THE ISOLATION FOREST ALGORITHM BASED ON AUTHENTICATION LOG FEATURE ANALYSIS

Password Spraying is a security threat that is difficult to detect because the attacker attempts a small number of common passwords against many accounts, making the activity resemble ordinary login failures and avoiding account lockout mechanisms. The problem addressed in this research is how to build a system that can log authentication activity and detect Password Spraying attacks in realtime. This research aims to build an authentication activity logging system and to implement the Isolation Forest algorithm to detect such attacks based on the analysis of authentication log features. The research stages include designing the logging system, labeling data by grouping activities within a one-minute time window, and training the model using a semi-supervised approach, in which the model is trained only on normal-labeled data. Testing was conducted on a simulated dataset of 4,213 records using three training-testing split scenarios, namely 70:30, 80:20, and 90:10. In the 80:20 scenario, the model achieved an accuracy of 96.44%, an ROC-AUC of 0.9581, and a recall of 1.00 for the attack class, meaning that all Password Spraying attacks in the test data were detected without any being missed. Thus, it can be concluded that the Isolation Forest algorithm can be applied to detect Password Spraying attacks in realtime based on authentication log features.

Keywords: Password Spraying, Isolation Forest, authentication log, semi-supervised, realtime

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Deteksi Serangan Password Spraying Secara Realtime Menggunakan Algoritma Isolation Forest Berdasarkan Analisis Fitur Log Autentikasi" ini dengan baik.

Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan studi pada Program Studi Sistem Komputer, Fakultas Ilmu Komputer dan Science, Universitas Indo Global Mandiri. Selama proses penyusunannya, penulis banyak mendapatkan bimbingan, masukan, serta dukungan dari berbagai pihak, sehingga skripsi ini dapat diselesaikan dengan baik.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Dr. H. Marzuki Alie, S.E., M.M., selaku Rektor Universitas Indo Global Mandiri, atas kesempatan yang diberikan kepada penulis untuk menempuh pendidikan di universitas ini.
2. Bapak Dr. Herri Setiawan, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer dan Science, atas dukungan dan fasilitas yang diberikan selama masa perkuliahan.
3. Bapak Tasmi, S.Si., M.Kom., selaku Ketua Program Studi (Kaprodi) Sistem Komputer sekaligus Dosen Pembimbing II, atas arahan, masukan, dan koreksi yang membantu penulis menyelesaikan skripsi ini dengan lebih terarah.
4. Bapak Ferdiansyah, S.Kom., M.Kom., Ph.D., selaku Dosen Pembimbing I, atas waktu, bimbingan, serta arahan yang diberikan sejak awal hingga akhir penyusunan skripsi ini.
5. Seluruh dosen dan staf Program Studi Sistem Komputer Universitas Indo Global Mandiri, atas ilmu dan pengalaman yang diberikan selama masa perkuliahan.
6. Orang tua dan keluarga penulis, atas doa, dukungan, dan kesabaran yang tidak pernah putus selama penulis menempuh pendidikan.

7. Rekan-rekan mahasiswa Program Studi Sistem Komputer, atas diskusi, bantuan, dan semangat yang diberikan selama masa perkuliahan hingga penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dan memiliki keterbatasan, baik dari segi penulisan maupun substansi. Penulis membuka diri terhadap kritik dan saran yang membangun agar penelitian ini dapat dikembangkan lebih lanjut. Akhir kata, penulis berharap skripsi ini dapat bermanfaat, khususnya bagi pengembangan keilmuan di bidang keamanan sistem dan deteksi anomali pada log autentikasi.

Palembang, 20 Juli 2026

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR LAMPIRAN