ANALISIS ANCAMAN KEAMANAN DIGITAL AKIBAT PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM SERANGAN SIBER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 - Informatika

disusun oleh

SHELVIA MAGHDALENA PUTRI

22.11.5050

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

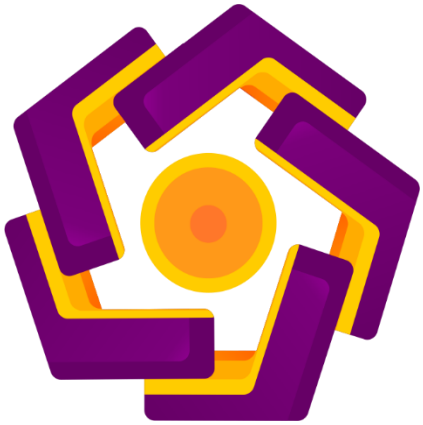
2026

ANALISIS ANCAMAN KEAMANAN DIGITAL AKIBAT PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM SERANGAN SIBER

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 - Informatika



disusun oleh

SHELVIA MAGHDALENA PUTRI

22.11.5050

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS ANCAMAN KEAMANAN DIGITAL AKIBAT PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM SERANGAN SIBER

yang disusun dan diajukan oleh
Shelvia Maghdalena Putri
22.11.5050

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal < 26 Januari 2026 >

Dosen Pembimbing,

Bayu Setiaji, M. Kom.
NIK. 190302216

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS ANCAMAN KEAMANAN DIGITAL AKIBAT PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE DALAM SERANGAN SIBER

yang disusun dan diajukan oleh
Shelvia Maghdalena Putri
22.11.5050
Telah dipertahankan di depan Dewan Penguji
pada tanggal < 26 Januari 2026 >
Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Mujiyanto, M.Kom **NIK. 190302492**	
Agung Pambudi, S.T., M.A. **NIK. 190302012**	
Bayu Setiaji, M.Kom. **NIK. 190302216**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal < 26 Januari 2026 >

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Shelvia Maghdalena Putri
NIM : 22.11.5050

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Ancaman Keamanan Digital akibat Penyalahgunaan Artificial Intelligence dalam Serangan Siber

Dosen Pembimbing : Bayu Setiaji, M. Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, < 26 Januari 2026 >
Yang Menyatakan,

Shelvia Maghdalena Putri

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahkan kepada:

1. Allah SWT, atas segala limpahan rahmat, hidayah, dan kekuatan yang diberikan-Nya, sehingga penulis mampu melewati setiap tantangan dalam penyusunan skripsi ini hingga tuntas.
2. Ayahanda Ayep Suryani dan Ibunda Peni Lestari, kedua orang tuaku tercinta, pahlawan hidupku yang tidak pernah lelah memberikan doa terbaik, dukungan material, serta kasih sayang tak terhingga. Terima kasih telah menjadi alasan terkuat penulis untuk terus berjuang dan menyelesaikan pendidikan ini.
3. Adik-adikku tercinta, Almiski Bintang Marindra, Muhamad Ahza Pradipta, Jaris Aditya Lesmana, terima kasih atas doa, dukungan, dan pengertiannya selama ini. Terima kasih sudah mengalah dan memahami kesibukan kakak. Sukses ini juga untuk kalian.
4. Teruntuk dirimu Mantri Kromo Fandith Fili, terima kasih atas segala dukungan dan *support*-nya selama ini. Terima kasih sudah selalu ada dan meyakinkan kalau aku bisa menyelesaikan ini.
5. Keluarga besar penulis, yang selalu memberikan semangat dan dukungan dalam setiap tahap perjalanan akademik.
6. Dosen pembimbing Bapak Bayu Setiaji, M. Kom dan seluruh dosen Program Studi S1 Informatika Universitas AMIKOM Yogyakarta, atas ilmu, bimbingan, serta arahan yang telah diberikan.
7. Teman-teman dan Almamaterku Terima kasih Universitas AMIKOM Yogyakarta dan kawan-kawan seperjuangan. Kalian adalah warna indah dalam masa mudaku.

Semoga skripsi ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Analisis Ancaman Keamanan Digital Akibat Penyalahgunaan Artificial Intelligence dalam Serangan Siber"** dengan baik.

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta. Penulis menyadari bahwa proses penyusunan skripsi ini melibatkan banyak tantangan, namun berkat bantuan, bimbingan, dan dukungan dari berbagai pihak, segala hambatan tersebut dapat teratasi.

Oleh karena itu, dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih yang setulus-tulusnya kepada:

1. Bapak Prof. Dr. Kusrini, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
2. Bapak Bayu Setiaji, M.Kom., selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, arahan, serta masukan yang sangat berharga sejak awal hingga selesainya penyusunan skripsi ini.
3. Bapak dan Ibu Dosen Program Studi S1 Informatika Universitas AMIKOM Yogyakarta, terima kasih atas ilmu pengetahuan dan wawasan yang telah diberikan selama penulis menempuh pendidikan.
4. Kedua Orang Tua dan Keluarga tercinta, yang senantiasa memberikan doa tulus, kasih sayang, dukungan moral maupun materiel, serta motivasi tanpa henti yang menjadi kekuatan utama bagi penulis.
5. Seluruh Responden, Sahabat, dan Teman-teman seperjuangan yang telah bersedia meluangkan waktu untuk membantu pengumpulan data, memberikan semangat, serta berbagi diskusi selama proses penelitian ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna karena keterbatasan pengetahuan dan pengalaman penulis. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi penyempurnaan di masa mendatang.

Akhir kata, semoga skripsi ini dapat memberikan manfaat bagi pembaca, serta dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Yogyakarta, 26 Januari 2026
Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI viii
DAFTAR TABEL xi
DAFTAR GAMBAR xii
INTISARI xiii
ABSTRACT xiv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 5
BAB II TINJAUAN PUSTAKA 6
2.1 Studi Literatur 6
2.2 Dasar Teori 17
2.2.1 Keamanan Digital 17
2.2.2 Kecerdasan Buatan (*Artificial Intelligence*) 18
2.2.3 Kerangka Konseptual Penelitian 19

BAB III METODE PENELITIAN 20
3.1 Objek Penelitian 20
3.2 Alur Penelitian 20
3.3 Alat dan Bahan 23
3.3.1 Data Penelitan 23
3.3.2 Alat dan Instrumen Penelitian 24
3.4 Kuesioner 26
BAB IV HASIL DAN PEMBAHASAN 32
4.1 Gambaran Umum Objek Penelitian 32
4.2 Hasil Studi Literatur 32
4.2.1 Bentuk Penyalahgunaan AI 32
4.2.2 Temuan Penting dari Literatur 33
4.2.3 Kesimpulan Studi Literatur 35
4.3 Hasil Kuesioner 36
4.3.1 Profile Responden 36
4.3.2 Tingkat Kesadaran terhadap Ancaman AI 37
4.3.3 Persepsi Dampak terhadap CIA *Triad* 38
4.3.4 Gap: Ancaman vs Efektivitas Deteksi 39
4.3.5 Status Kesiapan Organisasi 40
4.3.6 Tantangan Utama Organisasi 41
4.4 Hasil Eksperimen Simulasi Serangan Berbasis AI 41
4.4.1 Eksperimen 1: *AI-Powered Phishing Attack* 41
4.4.2 Eksperimen 2: Deteksi Manipulasi Wajah (*Deepfake*) 44
4.4.3 Eksperimen 3: Pengujian Respons Sistem Keamanan Jaringan 48
4.5 Triangulasi Data dan Pembahasan 53
4.5.1 Validasi Ancaman Kerahasiaan (*Confidentiality*) 54

4.5.2 Validasi Ancaman Integritas (*Integrity*) akibat *Deepfake* 54
4.5.3 Kesenjangan Deteksi (*The Detection Gap*) 55
4.5.4 Rangkuman Pembahasan 56
4.6 Analisis Data Survei (Persepsi Dampak) 56
4.7 Analisis Dampak Terhadap Keamanan Informasi (CIA *Triad*) 57
4.7.1 Dampak terhadap *Confidentiality* (Kerahasiaan) 57
4.7.2 Dampak terhadap *Integrity* (Integritas) 58
4.7.3 Dampak terhadap *Availability* (Ketersediaan) 58
4.8 Implikasi dan Strategi Mitigasi 58
4.8.1 Transformasi Menuju Deteksi Cerdas Berbasis AI 59
4.8.2 Penguatan Respons Insiden Otomatis (*Automated Response*) 59
4.8.3 Penerapan Analisis Forensik Berkelanjutan 59
BAB V PENUTUP 60
5.1 Kesimpulan 60
5.2 Saran 61
REFERENSI 63

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian 9
Tabel 3. 1 Alat Perangkat Keras Penelitian 22
Tabel 3. 2 Alat Perangkat Lunak Penelitian 22
Tabel 3. 3 *Dataset* Penelitian 23
Tabel 3. 4 Instrumen Penelitian 23
Tabel 4. 1 Sumber Data Penelitian 30
Tabel 4. 2 Bentuk Penyalahgunaan AI 30
Tabel 4. 3 Komparasi Efektivitas Serangan AI vs Konvensional 31
Tabel 4. 4 Dampak AI terhadap CIA *Triad* Berdasarkan Literatur 32
Tabel 4. 5 Keterbatasan Sistem Keamanan Tradisional 33
Tabel 4. 6 Karakteristik Demografi Responden (N=45) 34
Tabel 4. 7 Awareness dan Pengalaman Responden 36
Tabel 4. 8 Skor Dampak CIA *Triad* (Skala Likert 1-5) 36
Tabel 4. 9 Kesenjangan Proyeksi Ancaman dan Kesiapan Pertahanan 37
Tabel 4. 10 Kematangan Strategi Keamanan AI 38
Tabel 4. 11 Adopsi Teknologi Keamanan (Multiple Response) 38
Tabel 4. 12 Top 6 Tantangan 39
Tabel 4. 13 Triangulasi Data 52
Tabel 4. 14 Rekapitulasi Skor Persepsi Responden terhadap Lanskap Ancaman (Sumber: Olahan Data Primer, 2025) 55

DAFTAR GAMBAR

Gambar 3. 1 Alur Penelitian..... 19
Gambar 4. 1 Perbandingan Tingkat Kerapian Tata Bahasa (Grammar Clean) antar Tipe Emai..... 41
Gambar 4. 2 *Confusion matrix* Hasil Klasifikasi Serangan 42
Gambar 4. 3 Grafik *Feature importance* pada Deteksi *Phishing*..... 43
Gambar 4. 4 Distribusi *Dataset Deepfake*: Keseimbangan Kelas *Real* vs *Fake*... 44
Gambar 4. 5 *Confusion matrix* Hasil Deteksi *Deepfake* pada Data Uji 45
Gambar 4. 6 Skema Topologi Jaringan *Host*-to-*Guest* pada Eksperimen *Snort* IDS 48
Gambar 4. 7 Eksekusi Script Serangan *SQL Injection* dan Traversal dari Sisi Penyerang..... 50
Gambar 4. 8 Log Deteksi Serangan pada /var/log/*Snort*/alert 50
Gambar 4. 9 Persepsi Responden terhadap Dampak Serangan Siber 54

INTISARI

Perkembangan teknologi *Artificial Intelligence* (AI) menciptakan celah keamanan baru yang dieksploitasi untuk serangan siber yang lebih canggih dan adaptif. Penelitian ini bertujuan menganalisis ancaman keamanan digital akibat penyalahgunaan AI, mengidentifikasi dampaknya terhadap CIA *Triad* (*Confidentiality*, *Integrity*, *Availability*), serta merumuskan strategi mitigasi yang efektif. Metode penelitian menggunakan pendekatan *mixed-method* dengan kombinasi studi literatur sistematis, survei terhadap 45 praktisi keamanan siber dan profesional IT, serta eksperimen teknis terkontrol meliputi simulasi AI-*powered phishing*, deteksi *deepfake* menggunakan arsitektur Xception, dan pengujian *Intrusion Detection System* (*Snort*). Hasil penelitian menunjukkan serangan *phishing* berbasis AI memiliki tingkat kerapian grammar mendekati email legitimate (skor 1.0), meningkatkan kesulitan deteksi hingga 45% dibandingkan metode konvensional. Model deteksi *deepfake* mencapai akurasi 94% dengan arsitektur Xception. Survei menunjukkan praktisi menilai dampak terhadap kerahasiaan (4.56/5) dan integritas (4.40/5) sebagai ancaman paling kritis, namun efektivitas alat deteksi saat ini hanya dinilai moderat (3.33/5), mengindikasikan kesenjangan signifikan. Penelitian merekomendasikan transformasi menuju deteksi cerdas berbasis *Machine Learning*, penguatan respons insiden otomatis, dan penerapan analisis forensik berkelanjutan. Kontribusi penelitian meliputi identifikasi spesifik enam bentuk penyalahgunaan AI, analisis dampak kuantitatif berdasarkan data empiris, dan roadmap implementasi praktis untuk meningkatkan postur keamanan organisasi menghadapi era ancaman siber berbasis AI.

Kata kunci: *Artificial Intelligence, keamanan siber, deepfake, phishing, Intrusion Detection System.*

ABSTRACT

The advancement of Artificial Intelligence (AI) technology has created new security vulnerabilities exploited for more sophisticated and adaptive cyberattacks. This research aims to analyze digital security threats arising from AI misuse in cyberattacks, identify their impact on the CIA Triad (Confidentiality, Integrity, Availability), and formulate effective mitigation strategies. The research methodology employs a mixed-method approach combining systematic literature review, surveys of 45 cybersecurity practitioners and IT professionals, and controlled technical experiments including AI-powered phishing simulation, deepfake detection using Xception architecture, and Intrusion Detection System (Snort) response testing. Results demonstrate that AI-based phishing attacks exhibit grammar cleanliness scores approaching legitimate emails (1.0), increasing detection difficulty by 45% compared to conventional methods. The deepfake detection model achieved 94% accuracy with Xception architecture. Survey data reveal practitioners assess Confidentiality impact (4.56/5) and Integrity impact (4.40/5) as the most critical threats, yet current detection tool effectiveness is rated only moderate (3.33/5), indicating a significant gap. This research recommends transformation toward intelligent Machine Learning-based detection, strengthening automated incident response, and implementing continuous forensic analysis. Research contributions include specific identification of six forms of AI misuse, quantitative impact analysis based on empirical data, and practical implementation roadmap for enhancing organizational security posture in the era of AI-based cyber threats.

Keyword: *Artificial Intelligence, cybersecurity, deepfake, phishing, Intrusion Detection System.*