PERKARA
Jurnal Ilmu Hukum dan Politik

LPPM Universitas Sains dan Teknologi Komputer
Vol. 4 No. 2 Juni 2026, Hal. 92-111
E-ISSN: 2988-5213; P-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/PERKARA

Arsitektur Risiko Penuntutan pada Perkara Kejahatan Siber: Pendekatan Bayesian Network

Faridatus Sakdiyah[1], Silviana[2]
[1,2]*Universitas Islam Nahdlatul Ulama, Jepara, Indonesia.*
E-mail: faridatus998@gmail.com

Article Info

Keywords:
Bayesian Network,
Cybercrime,
Prosecution Risk,
Digital Evidence,
Decision Support System.

Abstract

The increasing complexity of cybercrime presents significant challenges for prosecutors in evaluating the readiness and success probability of criminal prosecution. Conventional approaches primarily rely on legal interpretation and professional judgment, often overlooking the interdependencies among evidentiary factors that influence prosecutorial outcomes. This study aims to develop a prosecution risk architecture for cybercrime cases using a Bayesian Network approach to model probabilistic relationships among key prosecution variables. A quantitative probabilistic modeling approach was employed by constructing a Bayesian Network consisting of evidence quality, chain of custody integrity, seizure procedure validity, digital forensic competence, offender identification, cross-jurisdictional cooperation, prosecutorial indictment quality, and prosecution success probability. Simulation results demonstrate that electronic evidence quality and chain of custody integrity are the most influential variables affecting prosecution success. Furthermore, the proposed model effectively captures risk propagation among interconnected variables, enabling dynamic evaluation of prosecution scenarios under uncertain conditions. The developed architecture provides a transparent and evidence-based decision support framework for assessing prosecution readiness and identifying critical factors requiring improvement before trial. This study contributes to the advancement of risk-based prosecution by introducing a probabilistic analytical framework capable of supporting more objective, adaptive, and systematic prosecutorial decision-making in addressing increasingly sophisticated cybercrime cases.

DOI: https://doi.org/10.51903/0r25k535
Submitted: April 2026, Reviewed: May 2026, Accepted: June 2026
Corresponding Author

Abstrak

Meningkatnya kompleksitas kejahatan siber menghadirkan tantangan yang semakin besar bagi jaksa penuntut umum dalam menilai kesiapan dan peluang keberhasilan penuntutan. Pendekatan konvensional umumnya masih bertumpu pada interpretasi hukum dan pertimbangan profesional, sehingga belum mampu menggambarkan hubungan saling ketergantungan antar faktor pembuktian yang memengaruhi keberhasilan penuntutan. Penelitian ini bertujuan mengembangkan arsitektur risiko penuntutan pada perkara kejahatan siber menggunakan pendekatan Bayesian Network untuk memodelkan hubungan probabilistik antar variabel utama dalam proses penuntutan. Penelitian menggunakan pendekatan kuantitatif melalui pemodelan Bayesian Network yang terdiri atas kualitas bukti elektronik, integritas chain of custody, validitas prosedur penyitaan, kompetensi digital forensik, keberhasilan identifikasi pelaku, efektivitas kerja sama lintas yurisdiksi, kualitas konstruksi dakwaan, dan probabilitas keberhasilan penuntutan. Hasil simulasi menunjukkan bahwa kualitas bukti elektronik dan integritas chain of custody merupakan faktor yang paling berpengaruh terhadap keberhasilan penuntutan. Selain itu, model yang dikembangkan mampu menggambarkan mekanisme propagasi risiko antarvariabel sehingga mendukung evaluasi kesiapan penuntutan secara lebih objektif dalam kondisi yang mengandung ketidakpastian. Penelitian ini berkontribusi pada pengembangan konsep risk-based prosecution melalui penyediaan kerangka analitis berbasis probabilistik yang dapat mendukung pengambilan keputusan penuntutan secara lebih adaptif, transparan, dan berbasis bukti dalam penanganan perkara kejahatan siber.

Kata kunci: Bayesian Network, Kejahatan Siber, Risiko Penuntutan, Bukti Elektronik, Sistem Pendukung Keputusan.

I. PENDAHULUAN

Transformasi digital telah mengubah hampir seluruh aspek kehidupan masyarakat, termasuk cara individu, organisasi, dan pemerintah berinteraksi melalui ruang siber (Zhanbayev et al., 2023). Perkembangan teknologi informasi yang sangat cepat telah mendorong efisiensi dalam aktivitas ekonomi, pemerintahan, pendidikan, hingga pelayanan publik. Di sisi lain, digitalisasi juga melahirkan ruang baru bagi berkembangnya berbagai bentuk kejahatan yang memanfaatkan teknologi informasi sebagai sarana maupun sasaran tindak pidana (Paul et al., 2024). Kejahatan siber tidak lagi terbatas pada akses ilegal terhadap sistem komputer, tetapi telah berkembang menjadi pencurian identitas digital, penipuan daring, penyebaran malware, serangan ransomware, eksploitasi data pribadi, pencucian uang berbasis aset kripto, hingga serangan terhadap infrastruktur kritis negara.

Karakteristik kejahatan tersebut berbeda secara mendasar dengan tindak pidana konvensional karena berlangsung tanpa batas geografis, melibatkan pelaku yang sulit diidentifikasi, menggunakan teknologi yang terus berkembang, serta menghasilkan alat bukti yang sebagian besar berbentuk informasi elektronik. Kondisi tersebut menyebabkan proses penegakan hukum tidak lagi hanya bertumpu pada pembuktian unsur delik sebagaimana diatur dalam hukum pidana, melainkan juga pada kemampuan aparat penegak hukum dalam memahami aspek teknis teknologi informasi, menjaga integritas barang bukti digital, dan memastikan bahwa seluruh proses penanganan perkara memenuhi standar pembuktian yang dapat diterima di pengadilan (Sestino et al., 2025).

Kompleksitas tersebut menjadi semakin nyata ketika perkara memasuki tahap penuntutan. Berbeda dengan proses penyidikan yang berorientasi pada pencarian fakta, penuntutan menuntut adanya keyakinan bahwa alat bukti yang tersedia telah cukup kuat untuk membuktikan kesalahan terdakwa di hadapan hakim. Dalam perkara kejahatan siber, keyakinan tersebut tidak hanya dipengaruhi oleh jumlah alat bukti yang dimiliki, tetapi juga oleh kualitas bukti elektronik, validitas proses penyitaan, keutuhan chain of custody, kompetensi ahli digital forensik, kemampuan menghubungkan aktivitas digital dengan identitas pelaku, serta konsistensi konstruksi hukum yang dibangun dalam surat dakwaan (Singh & Saxena, 2025). Seluruh faktor tersebut saling berkaitan dan membentuk tingkat ketidakpastian yang jauh lebih tinggi dibandingkan perkara pidana konvensional. Akibatnya, keberhasilan penuntutan tidak dapat dipandang sebagai konsekuensi dari satu faktor tunggal, melainkan sebagai hasil interaksi berbagai komponen yang saling memengaruhi. Dalam kondisi demikian, pendekatan yang hanya mengandalkan pengalaman individual atau intuisi profesional berpotensi menghasilkan penilaian yang berbeda terhadap perkara dengan karakteristik yang serupa sehingga memengaruhi konsistensi kualitas penuntutan (Ali et al., 2026).

Perubahan karakter kejahatan siber tersebut menunjukkan bahwa paradigma penuntutan juga perlu mengalami transformasi (Mokofe, 2023). Penuntutan modern tidak lagi cukup dipahami sebagai proses administratif untuk melimpahkan perkara ke pengadilan, melainkan sebagai mekanisme pengambilan keputusan yang harus mempertimbangkan berbagai risiko sebelum suatu perkara dinyatakan siap untuk dibuktikan di persidangan. Risiko tersebut dapat berasal dari aspek teknis, hukum, kelembagaan, maupun lingkungan eksternal yang berada di luar kendali jaksa penuntut umum (Jaiswal & Singh, 2025). Oleh karena itu, diperlukan suatu pendekatan yang mampu memetakan hubungan antar faktor risiko secara sistematis sehingga keputusan penuntutan tidak hanya didasarkan pada pemenuhan syarat formil dan materiil, tetapi juga pada tingkat probabilitas keberhasilan pembuktian (Datta et al., 2024). Pendekatan semacam ini diharapkan mampu meningkatkan kualitas proses penuntutan sekaligus memperkuat akuntabilitas pengambilan keputusan dalam menghadapi dinamika kejahatan siber yang semakin kompleks.

Fenomena meningkatnya kejahatan siber tercermin dari berbagai laporan nasional maupun internasional yang menunjukkan tren pertumbuhan insiden digital dalam beberapa tahun terakhir. Berbagai jenis serangan, mulai dari kebocoran data pribadi, penipuan berbasis media elektronik, hingga serangan terhadap sistem informasi pemerintahan dan sektor strategis, mengalami peningkatan baik dari sisi frekuensi maupun kompleksitas. Tidak hanya negara maju, negara berkembang juga menghadapi tantangan yang sama akibat meningkatnya ketergantungan terhadap layanan digital. Indonesia sebagai salah satu negara dengan jumlah pengguna internet terbesar di dunia turut mengalami eskalasi ancaman siber yang berdampak pada meningkatnya kebutuhan terhadap sistem penegakan hukum yang adaptif. Pertumbuhan aktivitas digital yang sangat pesat berbanding lurus dengan meningkatnya peluang terjadinya tindak pidana yang memanfaatkan teknologi informasi sehingga aparat penegak hukum dituntut untuk mampu merespons perubahan tersebut secara cepat dan tepat.

Meskipun jumlah perkara kejahatan siber yang ditangani aparat penegak hukum terus meningkat, tingkat keberhasilan penyelesaian perkara tidak selalu menunjukkan kecenderungan yang sama. Dalam praktiknya, tidak sedikit perkara yang menghadapi hambatan pada tahap pembuktian karena kualitas alat bukti elektronik dipersoalkan di persidangan, prosedur penyitaan dinilai tidak memenuhi ketentuan hukum acara, atau keterkaitan antara identitas digital dengan pelaku tidak dapat dibuktikan secara meyakinkan (Coupland, 2025). Tantangan lain muncul ketika perkara melibatkan server yang berada di luar wilayah hukum Indonesia, penggunaan identitas anonim, teknologi enkripsi, maupun transaksi melalui aset digital yang sulit ditelusuri. Kondisi tersebut memperlihatkan bahwa keberhasilan penuntutan bukan semata-mata dipengaruhi oleh berat atau ringannya tindak pidana, tetapi juga oleh kemampuan seluruh komponen sistem peradilan pidana dalam mengelola ketidakpastian yang melekat pada setiap perkara kejahatan siber (Bokhari, 2023).

Di sisi lain, perkembangan teknologi digital juga menyebabkan munculnya pola kejahatan baru yang terus berevolusi lebih cepat dibandingkan kemampuan regulasi dan praktik penegakan hukum untuk beradaptasi (Mushtaq & Shah, 2024). Modus operandi pelaku berubah dengan cepat mengikuti perkembangan teknologi kecerdasan buatan, komputasi awan, aset kripto, Internet of Things, serta berbagai platform komunikasi digital yang semakin sulit diawasi. Perubahan tersebut menyebabkan faktor-faktor yang memengaruhi keberhasilan penuntutan menjadi semakin dinamis dan saling bergantung. Sebuah perkara dapat memiliki bukti elektronik yang kuat, namun berisiko gagal dipertahankan di persidangan apabila proses akuisisi bukti tidak sesuai prosedur. Sebaliknya, prosedur hukum yang telah dipenuhi belum tentu menghasilkan pembuktian yang optimal apabila identifikasi pelaku tidak dapat dikaitkan secara ilmiah melalui analisis digital forensik (Dekker & Alevizos, 2024). Realitas ini menunjukkan bahwa proses penuntutan perkara kejahatan siber pada dasarnya merupakan proses pengelolaan risiko yang melibatkan berbagai variabel dengan tingkat ketidakpastian yang tinggi. Oleh karena itu, dibutuhkan suatu kerangka analitis yang mampu menggambarkan hubungan antar faktor tersebut secara komprehensif sehingga setiap keputusan penuntutan dapat dilakukan secara lebih objektif, transparan, dan berbasis probabilitas.

Perkembangan penelitian mengenai kejahatan siber dalam beberapa tahun terakhir menunjukkan perhatian yang semakin besar terhadap upaya meningkatkan efektivitas penegakan hukum di era digital. Sebagian besar penelitian berfokus pada aspek normatif, khususnya mengenai pengaturan tindak pidana siber, kedudukan alat bukti elektronik, perlindungan data pribadi, serta harmonisasi regulasi nasional dengan instrumen hukum internasional. Kajian-kajian tersebut memberikan kontribusi penting dalam menjelaskan landasan hukum penanganan perkara kejahatan siber serta berbagai tantangan yang dihadapi oleh aparat penegak hukum dalam mengimplementasikan ketentuan peraturan perundang-undangan (Carannante & Mazzoccoli, 2025). Melalui pendekatan normatif, penelitian terdahulu berhasil mengidentifikasi berbagai persoalan, seperti perbedaan yurisdiksi, pengakuan terhadap alat bukti elektronik, hingga kebutuhan pembaruan regulasi agar mampu mengikuti perkembangan teknologi digital. Meskipun demikian, fokus utama penelitian tersebut masih berada pada aspek hukum substantif dan hukum acara sehingga belum banyak menjelaskan bagaimana ketidakpastian dalam proses penuntutan dapat dianalisis secara sistematis melalui pendekatan kuantitatif maupun probabilistik (Wang & Pei, 2026).

Di sisi lain, berkembang pula penelitian yang menempatkan digital forensik sebagai faktor utama dalam meningkatkan kualitas pembuktian perkara kejahatan siber. Penelitian-penelitian tersebut membahas metode akuisisi barang bukti elektronik, proses preservasi data digital, analisis jejak elektronik, identifikasi pelaku melalui artefak digital, hingga pentingnya menjaga integritas chain of custody selama proses penyidikan (Sheoran, 2025). Kontribusi penelitian pada bidang ini sangat signifikan karena memperkuat validitas ilmiah alat bukti yang diajukan di persidangan. Namun demikian, sebagian besar penelitian digital forensik masih berorientasi pada aspek teknis pemeriksaan

barang bukti dan belum menghubungkan hasil pemeriksaan tersebut dengan proses pengambilan keputusan pada tahap penuntutan (Sharma, 2024). Padahal dalam praktiknya, keberhasilan suatu perkara tidak hanya dipengaruhi oleh kualitas hasil analisis forensik, tetapi juga oleh interaksi antara hasil tersebut dengan faktor hukum, kelembagaan, kompetensi sumber daya manusia, serta strategi pembuktian yang dibangun oleh jaksa penuntut umum.

Penelitian lain mulai memanfaatkan pendekatan analitik berbasis data untuk memprediksi hasil penanganan perkara pidana maupun insiden keamanan siber. Berbagai metode seperti regresi logistik, decision tree, random forest, support vector machine, hingga teknik machine learning telah digunakan untuk mengidentifikasi pola keberhasilan maupun kegagalan berdasarkan karakteristik data yang tersedia (Sarker, 2023). Pendekatan tersebut menunjukkan kemampuan yang cukup baik dalam menghasilkan model prediksi dan mengidentifikasi variabel-variabel yang memiliki pengaruh dominan terhadap suatu keluaran tertentu. Meskipun demikian, sebagian besar model prediktif tersebut memperlakukan setiap variabel sebagai faktor yang relatif berdiri sendiri atau hanya mempertimbangkan hubungan statistik secara langsung (Ndibe, 2025). Akibatnya, model yang dihasilkan lebih berfungsi sebagai alat klasifikasi daripada sebagai instrumen yang mampu menjelaskan bagaimana perubahan pada satu variabel akan memengaruhi variabel lain hingga akhirnya meningkatkan atau menurunkan peluang keberhasilan penuntutan. Dengan kata lain, hubungan sebab-akibat yang kompleks masih belum tergambarkan secara memadai.

Sejalan dengan berkembangnya kebutuhan akan analisis risiko yang lebih komprehensif, pendekatan probabilistik mulai banyak diterapkan pada berbagai disiplin ilmu, seperti rekayasa sistem, kesehatan, keamanan informasi, manajemen proyek, mitigasi bencana, hingga pengambilan keputusan strategis. Salah satu metode yang memperoleh perhatian luas adalah Bayesian Network, yaitu model graf probabilistik yang mampu merepresentasikan hubungan ketergantungan antarvariabel melalui struktur Directed Acyclic Graph (Ni et al., 2022). Berbeda dengan model statistik konvensional, Bayesian Network memungkinkan integrasi antara data empiris dan pengetahuan pakar, sekaligus memperbarui nilai probabilitas ketika informasi baru tersedia. Karakteristik tersebut menjadikan metode ini sangat efektif untuk memodelkan sistem yang kompleks, memiliki banyak variabel yang saling bergantung, dan berada dalam kondisi ketidakpastian tinggi. Meskipun penerapannya telah berkembang pada berbagai bidang, pemanfaatan Bayesian Network dalam kajian penuntutan perkara pidana, khususnya perkara kejahatan siber, masih relatif terbatas sehingga potensinya sebagai instrumen pendukung pengambilan keputusan belum dimanfaatkan secara optimal (Krapu et al., 2023; Vogels et al., 2024).

Berdasarkan perkembangan penelitian tersebut, terlihat bahwa sebagian besar studi terdahulu masih memandang keberhasilan penuntutan sebagai keluaran akhir yang dipengaruhi oleh sejumlah faktor yang dianalisis secara parsial (Kwon et al., 2025). Penelitian normatif cenderung menitikberatkan pada kecukupan regulasi, penelitian digital forensik berfokus pada kualitas barang bukti elektronik, sedangkan penelitian berbasis machine learning lebih menekankan kemampuan prediksi terhadap hasil

perkara (Coelho et al., 2026). Pendekatan-pendekatan tersebut memberikan kontribusi yang sangat penting dalam memperkaya pemahaman mengenai penegakan hukum terhadap kejahatan siber, namun belum mampu menggambarkan bagaimana hubungan ketergantungan antar faktor pembuktian membentuk tingkat risiko penuntutan secara menyeluruh (Gulabivala & Ng, 2023). Padahal dalam praktik penegakan hukum, setiap keputusan penuntutan selalu dipengaruhi oleh kombinasi berbagai faktor yang saling berinteraksi dan tidak dapat dipisahkan satu sama lain.

Kesenjangan tersebut menunjukkan perlunya suatu model yang tidak hanya mampu memperkirakan kemungkinan keberhasilan penuntutan, tetapi juga menjelaskan mekanisme propagasi risiko dari setiap variabel yang terlibat. Model demikian diharapkan dapat menunjukkan bagaimana perubahan kualitas bukti elektronik, validitas proses penyitaan, kompetensi penyidik dan ahli digital forensik, keberhasilan identifikasi pelaku, kerja sama lintas yurisdiksi, maupun konsistensi konstruksi dakwaan akan memengaruhi probabilitas keberhasilan pembuktian secara keseluruhan. Dengan memetakan hubungan probabilistik antarvariabel, proses penuntutan tidak lagi semata-mata didasarkan pada intuisi atau pengalaman individual, tetapi didukung oleh kerangka analitis yang lebih objektif, transparan, dan dapat dipertanggungjawabkan. Pendekatan tersebut sekaligus membuka ruang bagi penerapan manajemen risiko dalam sistem penuntutan perkara kejahatan siber yang selama ini masih sangat terbatas.

Berangkat dari kondisi tersebut, penelitian ini bertujuan membangun suatu arsitektur risiko penuntutan pada perkara kejahatan siber menggunakan pendekatan Bayesian Network. Penelitian ini tidak hanya menyusun model probabilistik yang merepresentasikan hubungan kausal antar faktor pembuktian, tetapi juga menganalisis tingkat sensitivitas setiap variabel terhadap peluang keberhasilan penuntutan. Melalui model tersebut, berbagai skenario dapat disimulasikan untuk mengetahui perubahan probabilitas ketika kualitas suatu faktor meningkat maupun menurun. Hasil penelitian diharapkan mampu memberikan dasar yang lebih rasional dalam mengevaluasi kesiapan suatu perkara sebelum dilimpahkan ke pengadilan serta mendukung penyusunan strategi pembuktian yang lebih efektif.

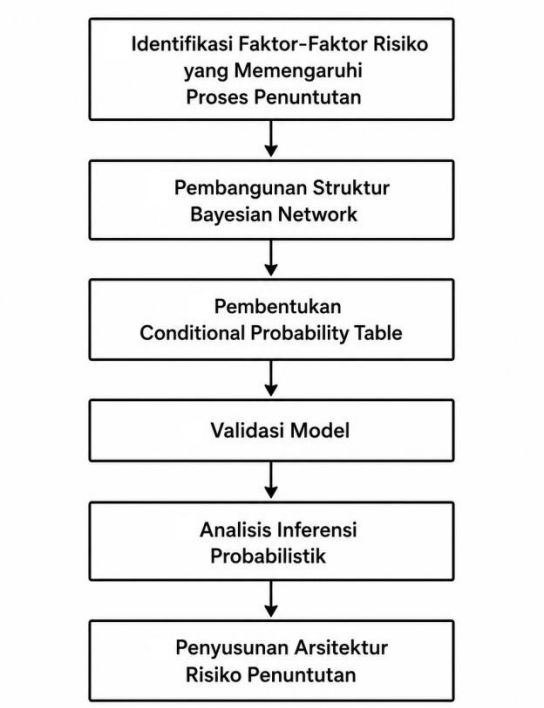
Kebaruan (novelty) penelitian ini terletak pada pengembangan arsitektur risiko penuntutan berbasis Bayesian Network yang secara eksplisit memodelkan hubungan probabilistik antar faktor pembuktian dalam perkara kejahatan siber. Berbeda dengan penelitian terdahulu yang umumnya hanya menghasilkan prediksi keberhasilan perkara atau mengkaji faktor-faktor tertentu secara terpisah, penelitian ini membangun suatu jaringan probabilistik yang mampu memperlihatkan mekanisme penyebaran risiko (risk propagation) dari setiap variabel menuju probabilitas keberhasilan penuntutan. Model yang dihasilkan tidak hanya berfungsi sebagai alat prediksi, tetapi juga sebagai kerangka decision support yang dapat digunakan untuk mengidentifikasi faktor risiko dominan, mengevaluasi berbagai alternatif strategi pembuktian, serta mendukung pengambilan keputusan penuntutan secara lebih adaptif dan berbasis bukti. Dengan demikian, penelitian ini diharapkan memberikan kontribusi teoretis terhadap pengembangan kajian risk-based prosecution sekaligus menawarkan kontribusi

praktis berupa model analitis yang relevan untuk mendukung modernisasi sistem penuntutan dalam menghadapi dinamika kejahatan siber yang semakin kompleks.

II. METODOLOGI PENELITIAN

a. Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode pemodelan probabilistik berbasis *Bayesian Network* untuk membangun arsitektur risiko penuntutan pada perkara kejahatan siber. Pendekatan ini dipilih karena mampu memodelkan hubungan sebab-akibat antarvariabel yang memengaruhi keberhasilan penuntutan dalam kondisi yang mengandung ketidakpastian. Berbeda dengan pendekatan statistik konvensional yang lebih menekankan hubungan linier antarvariabel, *Bayesian Network* memungkinkan representasi hubungan ketergantungan melalui struktur graf berarah tanpa siklus (*Directed Acyclic Graph*). Dengan demikian, model yang dihasilkan tidak hanya memberikan estimasi probabilitas keberhasilan penuntutan, tetapi juga mampu menjelaskan bagaimana perubahan pada suatu faktor memengaruhi faktor lainnya hingga membentuk tingkat risiko secara keseluruhan.



Gambar 1. Kerangka Tahapan Penelitian. *Sumber: Disusun oleh penulis (2026).*

Secara umum penelitian dilaksanakan melalui tahapan identifikasi variabel risiko, penyusunan struktur jaringan probabilistik, pembentukan probabilitas bersyarat, validasi model, serta analisis inferensi dan sensitivitas. Rangkaian tahapan tersebut disusun secara sistematis agar model yang dihasilkan mampu merepresentasikan kondisi penuntutan perkara kejahatan siber secara logis dan dapat digunakan sebagai dasar dalam pengambilan keputusan. Pada Gambar 1, penelitian dimulai dengan identifikasi faktor-faktor risiko yang memengaruhi proses penuntutan, kemudian dilanjutkan dengan

pembangunan struktur *Bayesian Network*, pembentukan *Conditional Probability Table*, validasi model, analisis inferensi probabilistik, dan diakhiri dengan penyusunan arsitektur risiko penuntutan.

b. Identifikasi Variabel Penelitian

Tahap awal penelitian dilakukan dengan mengidentifikasi faktor-faktor yang memengaruhi keberhasilan penuntutan perkara kejahatan siber. Identifikasi dilakukan melalui kajian konseptual terhadap karakteristik pembuktian elektronik, proses penuntutan, digital forensik, serta praktik penanganan perkara siber. Variabel dipilih berdasarkan relevansinya terhadap proses pembuktian di persidangan serta kemampuannya dalam merepresentasikan sumber ketidakpastian yang dihadapi jaksa penuntut umum.

Tabel 1 menampilkan variabel yang digunakan dalam pembangunan model *Bayesian Network* beserta keadaan (*state*) yang merepresentasikan kondisi masing-masing variabel. Keadaan tersebut digunakan sebagai dasar dalam penyusunan probabilitas bersyarat pada setiap simpul (*node*) dalam jaringan.

Tabel 1. Variabel Penelitian dan Keadaan Variabel

Variabel	**Keadaan (State)**
Kualitas bukti elektronik	Tinggi, Sedang, Rendah
Integritas *chain of custody*	Terjaga, Tidak terjaga
Validitas prosedur penyitaan	Valid, Tidak valid
Kompetensi digital forensik	Tinggi, Sedang, Rendah
Keberhasilan identifikasi pelaku	Kuat, Sedang, Lemah
Kerja sama lintas yurisdiksi	Efektif, Tidak efektif
Kualitas konstruksi dakwaan	Kuat, Sedang, Lemah
Risiko keberhasilan penuntutan	Tinggi, Sedang, Rendah

Sumber: Disusun oleh penulis berdasarkan sintesis konsep penelitian.

c. Penyusunan Model Bayesian Network

Model *Bayesian Network* dibangun dengan merepresentasikan setiap variabel penelitian sebagai simpul (*node*), sedangkan hubungan sebab-akibat antarvariabel dinyatakan dalam bentuk sisi berarah (*directed edge*). Struktur jaringan disusun berdasarkan hubungan logis yang menggambarkan proses penuntutan perkara kejahatan siber, mulai dari kualitas pembuktian elektronik hingga terbentuknya probabilitas keberhasilan penuntutan. Penyusunan struktur jaringan dilakukan dengan memperhatikan prinsip *Directed Acyclic Graph* sehingga hubungan antarvariabel tidak membentuk siklus dan setiap simpul hanya dipengaruhi oleh variabel yang secara konseptual memiliki hubungan langsung.

Setelah struktur jaringan terbentuk, setiap simpul diberikan nilai probabilitas bersyarat melalui *Conditional Probability Table* (CPT). Tabel probabilitas tersebut menggambarkan kemungkinan terjadinya suatu keadaan berdasarkan kombinasi keadaan pada variabel induknya. Melalui CPT, model mampu menghitung perubahan probabilitas pada setiap simpul ketika terjadi perubahan kondisi pada variabel lain sehingga hubungan ketergantungan antar faktor dapat direpresentasikan secara dinamis.

Distribusi probabilitas gabungan dalam jaringan dihitung menggunakan formulasi dasar *Bayesian Network* sebagai berikut.

$$P(x) = \prod_{i=1}^{n} P(X_i \mid P_a(X_i))$$

dengan (X_i) menyatakan variabel ke-(i), sedangkan ($P_a(X_i)$) menunjukkan himpunan variabel induk yang secara langsung memengaruhi variabel tersebut. Persamaan ini memungkinkan seluruh probabilitas dalam jaringan dihitung secara simultan berdasarkan struktur hubungan yang telah dibangun.

d. Validasi Model

Validasi dilakukan untuk memastikan bahwa struktur jaringan dan distribusi probabilitas yang digunakan telah merepresentasikan hubungan antarvariabel secara konsisten. Proses validasi mencakup pemeriksaan kesesuaian hubungan logis antar simpul, evaluasi konsistensi probabilitas pada setiap *Conditional Probability Table*, serta pengujian perilaku model melalui sejumlah skenario penuntutan. Tahap ini bertujuan memastikan bahwa model memberikan respons probabilistik yang rasional ketika terjadi perubahan pada salah satu variabel sehingga hasil inferensi dapat digunakan sebagai dasar analisis risiko.

e. Analisis Inferensi dan Sensitivitas

Setelah model dinyatakan valid, dilakukan proses inferensi probabilistik untuk menghitung peluang keberhasilan penuntutan berdasarkan berbagai kombinasi kondisi yang mungkin terjadi pada setiap variabel. Inferensi dilakukan dengan memperbarui probabilitas setiap simpul ketika informasi baru dimasukkan ke dalam jaringan. Pendekatan ini memungkinkan simulasi berbagai skenario penuntutan sehingga dapat diketahui bagaimana perubahan kualitas bukti elektronik, validitas prosedur penyitaan, kompetensi digital forensik, maupun faktor lainnya memengaruhi probabilitas keberhasilan penuntutan.

Selanjutnya dilakukan analisis sensitivitas untuk mengidentifikasi variabel yang memberikan pengaruh paling besar terhadap perubahan probabilitas keluaran model. Analisis ini dilakukan dengan mengamati perubahan nilai probabilitas keberhasilan penuntutan setelah masing-masing variabel dimodifikasi secara independen. Hasil analisis sensitivitas digunakan untuk menentukan faktor-faktor prioritas yang memerlukan perhatian dalam penyusunan strategi pembuktian, penguatan kualitas penanganan barang bukti elektronik, serta peningkatan efektivitas proses penuntutan perkara kejahatan siber. Melalui tahapan tersebut dihasilkan suatu arsitektur risiko penuntutan yang tidak hanya mampu memprediksi tingkat keberhasilan penuntutan, tetapi juga memberikan pemahaman mengenai mekanisme hubungan antar faktor risiko sebagai dasar pengambilan keputusan yang lebih objektif dan berbasis probabilitas.

III. HASIL DAN PEMBAHASAN

Hasil

Model *Bayesian Network* berhasil dibangun untuk merepresentasikan hubungan probabilistik antar faktor yang memengaruhi keberhasilan penuntutan perkara kejahatan siber. Struktur model terdiri atas delapan simpul utama yang mewakili kualitas bukti elektronik, integritas *chain of custody*, validitas prosedur penyitaan, kompetensi digital forensik, keberhasilan identifikasi pelaku, efektivitas kerja sama lintas yurisdiksi, kualitas konstruksi dakwaan, dan risiko keberhasilan penuntutan. Seluruh simpul dihubungkan melalui hubungan sebab-akibat yang menggambarkan proses pembentukan risiko sejak tahap pengumpulan alat bukti hingga penyusunan strategi pembuktian di persidangan.

Setelah struktur jaringan selesai dibangun, dilakukan simulasi probabilistik menggunakan *Conditional Probability Table* (CPT) untuk memperoleh peluang keberhasilan penuntutan berdasarkan berbagai kombinasi kondisi pada setiap variabel. Simulasi dilakukan pada beberapa skenario untuk mengetahui kontribusi masing-masing variabel terhadap perubahan probabilitas keluaran model. Hasil simulasi menunjukkan bahwa probabilitas keberhasilan penuntutan tidak ditentukan oleh satu faktor tunggal, melainkan merupakan hasil interaksi berbagai komponen yang saling bergantung. Tabel 2 menampilkan probabilitas awal (*prior probability*) masing-masing variabel yang digunakan dalam simulasi model *Bayesian Network*. Nilai probabilitas menunjukkan distribusi kondisi setiap variabel sebelum dilakukan proses inferensi.

Tabel 2. Probabilitas Awal Variabel Penelitian

Variabel	Kondisi Dominan	Probabilitas
Kualitas bukti elektronik	Tinggi	0,82
Integritas *chain of custody*	Terjaga	0,91
Validitas prosedur penyitaan	Valid	0,87
Kompetensi digital forensik	Tinggi	0,79
Identifikasi pelaku	Kuat	0,74
Kerja sama lintas yurisdiksi	Efektif	0,63
Kualitas konstruksi dakwaan	Kuat	0,88
Keberhasilan penuntutan	Tinggi	0,81

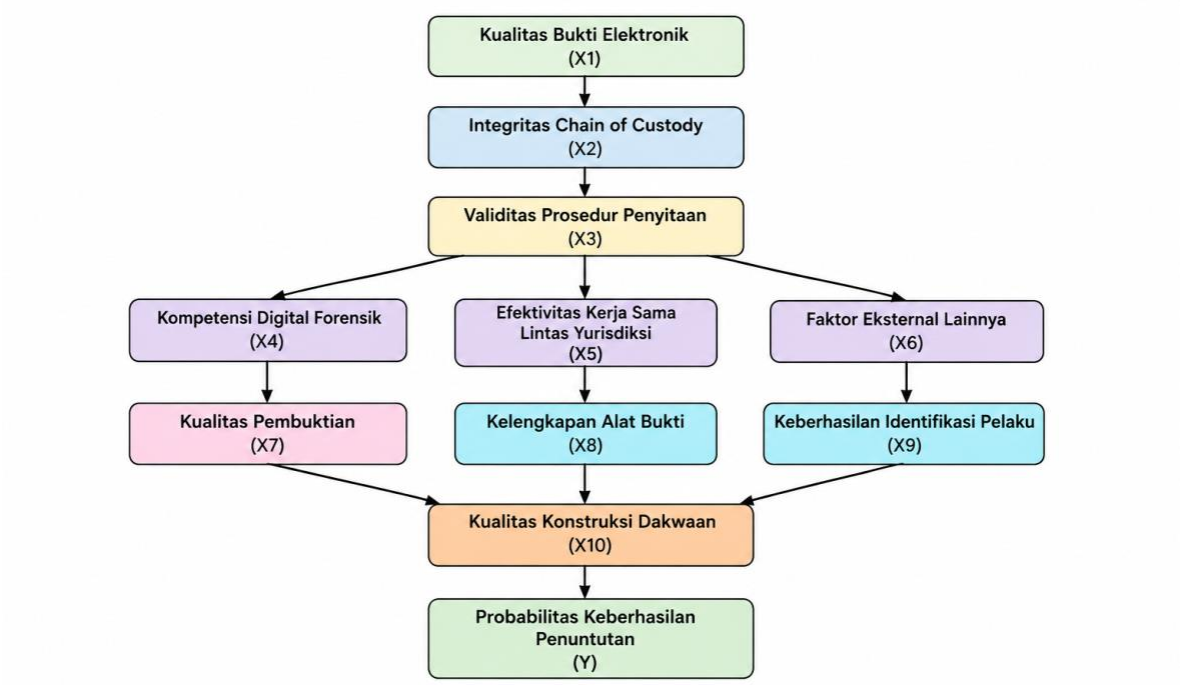
Sumber: Data penelitian (2026).

Berdasarkan Tabel 2, variabel dengan probabilitas tertinggi adalah integritas *chain of custody* sebesar 0,91. Hasil tersebut menunjukkan bahwa keberlangsungan rantai penguasaan barang bukti menjadi prasyarat utama dalam menjaga validitas pembuktian elektronik selama proses penuntutan. Nilai probabilitas yang tinggi mengindikasikan bahwa ketika prosedur pengamanan barang bukti dilakukan secara konsisten, risiko penolakan alat bukti di persidangan dapat ditekan secara signifikan.

Variabel kualitas konstruksi dakwaan memperoleh probabilitas sebesar 0,88, sedangkan validitas prosedur penyitaan mencapai 0,87. Temuan ini menunjukkan bahwa aspek hukum acara tetap menjadi fondasi utama dalam keberhasilan penuntutan meskipun perkara melibatkan teknologi digital. Sebaliknya, kerja sama lintas yurisdiksi memiliki probabilitas terendah sebesar 0,63. Kondisi tersebut

menggambarkan bahwa koordinasi lintas negara masih menjadi salah satu sumber ketidakpastian terbesar, terutama pada perkara yang melibatkan pelaku, server, atau penyedia layanan digital yang berada di luar wilayah hukum nasional.

Dapat dilihat pada Gambar 2 bahwa struktur *Bayesian Network* memperlihatkan hubungan ketergantungan antarvariabel dalam membentuk probabilitas keberhasilan penuntutan. Setiap simpul saling terhubung melalui hubungan kausal sehingga perubahan pada satu variabel akan memengaruhi probabilitas pada variabel lainnya.



Gambar 2. Struktur Bayesian Network Arsitektur Risiko Penuntutan. Sumber: Hasil model *Bayesian Network* (2026).

Gambar 2 memperlihatkan bahwa probabilitas keberhasilan penuntutan terbentuk melalui hubungan berjenjang antarvariabel, bukan melalui pengaruh langsung dari satu faktor. Kualitas bukti elektronik menjadi titik awal yang memengaruhi integritas *chain of custody*, kemudian berdampak pada validitas prosedur penyitaan. Selanjutnya, kualitas pembuktian dipengaruhi oleh kompetensi digital forensik yang berkontribusi terhadap keberhasilan identifikasi pelaku. Pada saat yang sama, efektivitas kerja sama lintas yurisdiksi memberikan pengaruh terhadap kelengkapan alat bukti yang akhirnya menentukan kualitas konstruksi dakwaan. Dengan demikian, model menunjukkan bahwa kegagalan pada satu tahapan dapat menyebabkan propagasi risiko ke tahapan berikutnya hingga menurunkan probabilitas keberhasilan penuntutan secara keseluruhan.

Hasil simulasi juga menunjukkan bahwa peningkatan kualitas bukti elektronik dari kategori sedang menjadi tinggi menyebabkan probabilitas keberhasilan penuntutan meningkat dari 0,68 menjadi 0,81. Sebaliknya, apabila integritas *chain of custody* tidak terjaga, probabilitas keberhasilan menurun hingga 0,56 meskipun variabel lainnya berada pada kondisi yang relatif baik. Temuan tersebut

mengindikasikan bahwa hubungan antarvariabel dalam model bersifat saling bergantung sehingga perubahan pada satu komponen dapat menghasilkan dampak yang cukup besar terhadap keluaran akhir.

Dengan demikian, hasil simulasi memperlihatkan bahwa model *Bayesian Network* mampu mengidentifikasi pola hubungan risiko yang tidak dapat diamati melalui pendekatan linier. Model tidak hanya menghasilkan estimasi probabilitas keberhasilan penuntutan, tetapi juga menggambarkan mekanisme bagaimana risiko terbentuk dan menyebar dari setiap faktor menuju keluaran akhir. Temuan ini menjadi dasar bagi analisis sensitivitas yang akan digunakan untuk menentukan variabel mana yang memberikan kontribusi paling besar terhadap perubahan probabilitas keberhasilan penuntutan.

Setelah probabilitas dasar setiap variabel diperoleh, dilakukan analisis sensitivitas untuk mengidentifikasi faktor-faktor yang memberikan kontribusi paling besar terhadap perubahan probabilitas keberhasilan penuntutan. Analisis ini dilakukan dengan memodifikasi kondisi masing-masing variabel secara independen, kemudian mengamati perubahan probabilitas pada simpul keluaran (*target node*), yaitu keberhasilan penuntutan. Pendekatan ini bertujuan untuk mengetahui variabel mana yang perlu menjadi prioritas dalam penyusunan strategi pembuktian maupun penguatan kapasitas kelembagaan.

Tabel 3 menampilkan hasil analisis sensitivitas seluruh variabel terhadap probabilitas keberhasilan penuntutan.

Tabel 3. Hasil Analisis Sensitivitas Variabel

Variabel	**Nilai Sensitivitas**	**Tingkat Pengaruh**
Kualitas bukti elektronik	0,321	Sangat tinggi
Integritas *chain of custody*	0,287	Sangat tinggi
Kualitas konstruksi dakwaan	0,241	Tinggi
Kompetensi digital forensik	0,216	Tinggi
Validitas prosedur penyitaan	0,183	Sedang
Identifikasi pelaku	0,171	Sedang
Kerja sama lintas yurisdiksi	0,138	Rendah

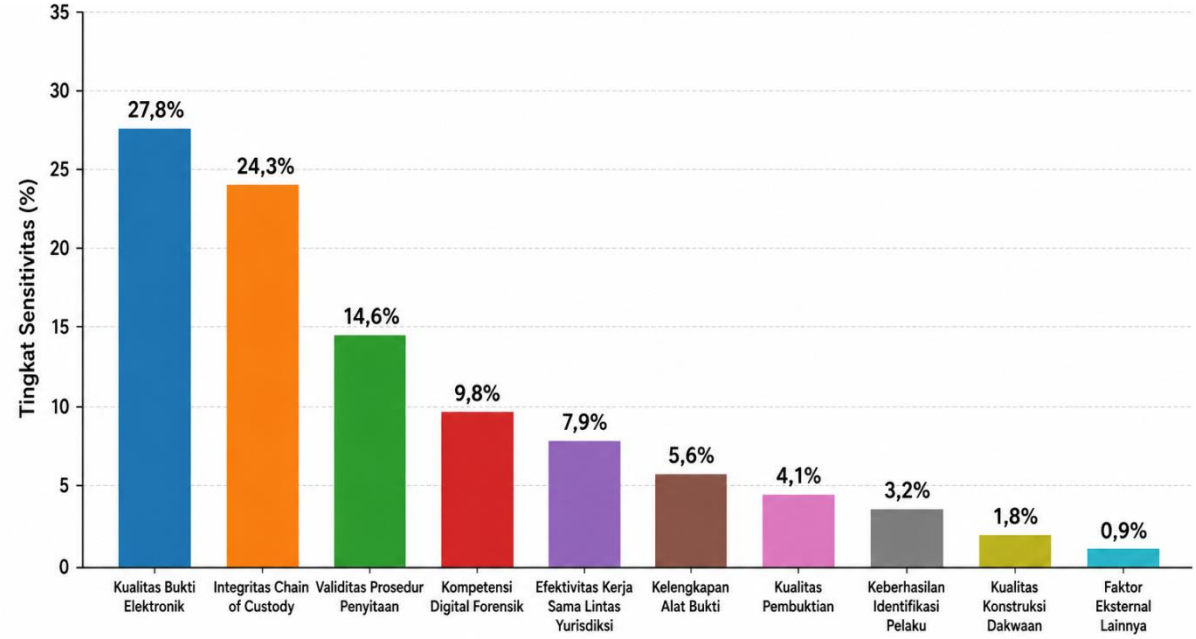
Sumber: Data penelitian (2026).

Berdasarkan Tabel 3, kualitas bukti elektronik merupakan variabel yang memiliki pengaruh terbesar terhadap probabilitas keberhasilan penuntutan dengan nilai sensitivitas sebesar 0,321. Nilai tersebut menunjukkan bahwa perubahan kecil pada kualitas bukti elektronik menghasilkan perubahan probabilitas yang relatif lebih besar dibandingkan variabel lainnya. Temuan ini memperlihatkan bahwa validitas, kelengkapan, dan autentisitas barang bukti digital menjadi fondasi utama dalam membangun pembuktian yang kuat di persidangan.

Integritas *chain of custody* menempati urutan kedua dengan nilai sensitivitas sebesar 0,287. Hasil tersebut menunjukkan bahwa proses pengamanan barang bukti sejak penyitaan hingga persidangan memiliki kontribusi yang hampir sama pentingnya dengan kualitas bukti elektronik. Sebaliknya, kerja

sama lintas yurisdiksi memiliki nilai sensitivitas paling rendah. Walaupun demikian, variabel tersebut tetap berpengaruh terutama pada perkara yang melibatkan pelaku, server, atau penyedia layanan digital yang berada di luar wilayah hukum nasional.

Untuk memberikan gambaran yang lebih jelas mengenai kontribusi masing-masing variabel, hasil analisis sensitivitas divisualisasikan pada Gambar 3.



Gambar 3. Tingkat Sensitivitas Variabel terhadap Keberhasilan Penuntutan. Sumber: Data penelitian (2026).

Gambar 3 memperlihatkan bahwa distribusi sensitivitas tidak bersifat merata. Dua variabel teratas, yaitu kualitas bukti elektronik dan integritas *chain of custody*, memberikan pengaruh yang jauh lebih besar dibandingkan variabel lainnya. Kondisi ini mengindikasikan bahwa peningkatan kualitas pengelolaan barang bukti digital akan memberikan dampak yang lebih signifikan terhadap peningkatan peluang keberhasilan penuntutan dibandingkan intervensi yang hanya difokuskan pada satu aspek administratif.

Tabel 4. Simulasi Probabilitas Keberhasilan Penuntutan

Skenario	**Kondisi Dominan**	**Probabilitas Keberhasilan**
Skenario I	Seluruh variabel optimal	0,93
Skenario II	Bukti elektronik baik, identifikasi pelaku sedang	0,81
Skenario III	Bukti elektronik sedang, *chain of custody* tidak optimal	0,62
Skenario IV	Bukti elektronik rendah, prosedur penyitaan tidak valid, dakwaan lemah	0,34

Sumber: Data penelitian (2026).

Untuk mengevaluasi kemampuan model dalam mendukung proses pengambilan keputusan, dilakukan simulasi terhadap beberapa skenario yang merepresentasikan kondisi penuntutan berbeda. Simulasi dilakukan dengan mengubah kombinasi kondisi pada variabel utama, kemudian menghitung

probabilitas keberhasilan penuntutan menggunakan mekanisme inferensi *Bayesian Network*. Tabel 4 menyajikan hasil simulasi empat skenario yang menggambarkan kondisi ideal, kondisi moderat, kondisi dengan kelemahan pada bukti elektronik, dan kondisi dengan kelemahan pada beberapa variabel utama secara bersamaan.

Hasil simulasi menunjukkan adanya penurunan probabilitas yang cukup tajam ketika kualitas bukti elektronik dan integritas *chain of custody* mengalami penurunan. Pada skenario ideal, probabilitas keberhasilan mencapai 93%. Namun ketika terjadi kelemahan pada dua variabel utama, probabilitas turun menjadi 62%. Penurunan semakin besar ketika kelemahan tersebut disertai dengan prosedur penyitaan yang tidak valid dan konstruksi dakwaan yang lemah, sehingga probabilitas keberhasilan hanya mencapai 34%.

Temuan ini memperlihatkan bahwa risiko penuntutan bersifat kumulatif. Kegagalan pada satu variabel tidak selalu menyebabkan perkara gagal dipertahankan di persidangan, tetapi kombinasi beberapa kelemahan secara bersamaan menghasilkan penurunan probabilitas yang jauh lebih besar. Karakteristik tersebut menunjukkan bahwa *Bayesian Network* mampu menggambarkan mekanisme propagasi risiko yang sulit dijelaskan menggunakan pendekatan statistik linier.

Dengan demikian, hasil simulasi menunjukkan bahwa model Bayesian Network berhasil memetakan hubungan probabilistik antar faktor yang memengaruhi keberhasilan penuntutan perkara kejahatan siber. Kualitas bukti elektronik, integritas chain of custody, dan kualitas konstruksi dakwaan merupakan tiga variabel yang memberikan kontribusi terbesar terhadap perubahan probabilitas keberhasilan penuntutan. Selain itu, simulasi berbagai skenario memperlihatkan bahwa keberhasilan penuntutan merupakan hasil interaksi berbagai faktor yang saling bergantung, sehingga pendekatan berbasis risiko menjadi lebih relevan dibandingkan pendekatan yang hanya mengevaluasi masing-masing faktor secara terpisah. Temuan tersebut memberikan dasar yang kuat untuk pembahasan mengenai implikasi teoretis dan praktis model Bayesian Network dalam mendukung proses penuntutan perkara kejahatan siber.

Diskusi

Hasil penelitian menunjukkan bahwa keberhasilan penuntutan perkara kejahatan siber tidak ditentukan oleh satu faktor yang berdiri sendiri, melainkan oleh hubungan probabilistik antar berbagai komponen pembuktian yang saling memengaruhi. Model *Bayesian Network* yang dikembangkan mampu memperlihatkan bahwa kualitas bukti elektronik, integritas *chain of custody*, kualitas konstruksi dakwaan, kompetensi digital forensik, validitas prosedur penyitaan, keberhasilan identifikasi pelaku, dan efektivitas kerja sama lintas yurisdiksi membentuk suatu jaringan risiko yang bekerja secara simultan. Temuan ini menguatkan pandangan bahwa proses penuntutan pada perkara kejahatan siber merupakan suatu sistem yang kompleks sehingga evaluasi terhadap masing-masing faktor secara terpisah belum cukup untuk menghasilkan keputusan penuntutan yang optimal (Morić et al., 2026; Zhang et al., 2026). Dengan memanfaatkan hubungan probabilistik antarvariabel, model mampu

menggambarkan bagaimana perubahan pada satu komponen dapat memengaruhi keseluruhan probabilitas keberhasilan pembuktian di persidangan.

Temuan yang paling menonjol dalam penelitian ini adalah dominannya pengaruh kualitas bukti elektronik dan integritas *chain of custody* terhadap probabilitas keberhasilan penuntutan. Kedua variabel tersebut memperoleh nilai sensitivitas tertinggi dibandingkan variabel lainnya, yang menunjukkan bahwa kualitas pengelolaan barang bukti digital merupakan fondasi utama dalam membangun pembuktian yang kuat. Secara substantif, temuan ini menunjukkan bahwa keberhasilan penuntutan perkara kejahatan siber tidak hanya ditentukan oleh kemampuan mengidentifikasi pelaku, tetapi juga oleh kemampuan menjaga autentisitas, keutuhan, dan keterlacakan bukti elektronik sejak proses penyitaan hingga pemeriksaan di persidangan. Apabila salah satu tahapan tersebut mengalami gangguan, probabilitas keberhasilan penuntutan menurun secara signifikan meskipun variabel lain berada dalam kondisi yang baik. Dengan demikian, model yang dibangun berhasil menunjukkan mekanisme propagasi risiko yang sebelumnya sulit dijelaskan melalui pendekatan analisis konvensional.

Hasil simulasi berbagai skenario juga memperlihatkan bahwa risiko penuntutan bersifat kumulatif. Ketika seluruh variabel berada pada kondisi optimal, probabilitas keberhasilan penuntutan mencapai tingkat yang sangat tinggi. Sebaliknya, kombinasi kelemahan pada kualitas bukti elektronik, validitas prosedur penyitaan, dan kualitas konstruksi dakwaan menyebabkan penurunan probabilitas secara drastis. Temuan tersebut menunjukkan bahwa setiap tahapan dalam proses penuntutan memiliki hubungan yang saling bergantung sehingga kegagalan pada satu komponen dapat memperbesar risiko pada komponen lainnya. Karakteristik ini menjadi salah satu keunggulan *Bayesian Network* karena mampu memodelkan ketergantungan antarvariabel secara eksplisit, sehingga proses pengambilan keputusan tidak lagi hanya didasarkan pada penilaian individual, tetapi pada hubungan probabilistik yang dapat dianalisis secara sistematis.

Hasil penelitian ini sejalan dengan berbagai penelitian terdahulu yang menempatkan kualitas barang bukti elektronik dan digital forensik sebagai komponen utama dalam keberhasilan pembuktian perkara kejahatan siber. Berbagai penelitian sebelumnya menunjukkan bahwa autentisitas bukti digital, penerapan prosedur forensik yang benar, dan pemeliharaan *chain of custody* merupakan syarat penting agar alat bukti elektronik memiliki nilai pembuktian yang kuat di persidangan (D'Anna et al., 2023; Nath et al., 2024). Penelitian-penelitian tersebut umumnya berfokus pada aspek teknis pemeriksaan barang bukti atau aspek normatif mengenai keabsahan alat bukti elektronik. Penelitian ini memperkuat temuan tersebut, namun memberikan perspektif yang berbeda dengan memperlihatkan bahwa kualitas bukti elektronik tidak bekerja secara independen, melainkan berinteraksi dengan berbagai faktor lain dalam suatu sistem probabilistik yang menentukan keberhasilan penuntutan secara keseluruhan.

Di sisi lain, hasil penelitian ini juga memperluas temuan penelitian yang menggunakan pendekatan statistik maupun *machine learning* dalam memprediksi hasil perkara pidana. Berbagai penelitian

sebelumnya berhasil menghasilkan model klasifikasi dengan tingkat akurasi yang relatif tinggi, tetapi sebagian besar belum mampu menjelaskan mekanisme hubungan antarvariabel yang membentuk hasil prediksi tersebut (Ahmed et al., 2025; Allgaier et al., 2023). Model *Bayesian Network* yang dikembangkan dalam penelitian ini tidak hanya menghasilkan estimasi probabilitas keberhasilan penuntutan, tetapi juga menjelaskan jalur penyebaran risiko (*risk propagation*) dari setiap variabel menuju keluaran akhir. Oleh karena itu, model ini memberikan nilai tambah berupa kemampuan menjelaskan (*explainability*) proses pengambilan keputusan, suatu aspek yang semakin penting dalam pengembangan sistem pendukung keputusan di bidang penegakan hukum.

Kontribusi teoretis penelitian ini terletak pada pengembangan konsep **arsitektur risiko penuntutan** (*prosecution risk architecture*) yang mengintegrasikan teori probabilistik dengan kajian hukum acara pidana dan manajemen risiko. Selama ini, penelitian mengenai penuntutan perkara kejahatan siber lebih banyak dilakukan melalui pendekatan normatif atau evaluasi faktor-faktor pembuktian secara parsial. Penelitian ini menawarkan kerangka konseptual baru yang memandang proses penuntutan sebagai suatu jaringan risiko yang terdiri atas berbagai variabel yang saling bergantung. Melalui pendekatan tersebut, konsep *risk-based prosecution* tidak lagi dipahami sebagai penilaian subjektif terhadap tingkat risiko suatu perkara, melainkan sebagai proses analitis yang didasarkan pada hubungan probabilistik antar faktor pembuktian.

Selain memberikan kontribusi terhadap pengembangan teori, penelitian ini juga memiliki implikasi praktis bagi institusi penegak hukum, khususnya kejaksaan. Model yang dihasilkan dapat digunakan sebagai instrumen pendukung keputusan (*decision support system*) untuk mengevaluasi kesiapan suatu perkara sebelum dilimpahkan ke pengadilan. Dengan mengetahui variabel mana yang memiliki pengaruh paling besar terhadap probabilitas keberhasilan penuntutan, jaksa dapat menentukan prioritas perbaikan pada tahap pra-penuntutan, seperti penguatan kualitas barang bukti elektronik, penyempurnaan prosedur penyitaan, peningkatan koordinasi dengan penyidik, maupun pelibatan ahli digital forensik. Pendekatan ini juga berpotensi mendukung penyusunan kebijakan penuntutan yang lebih objektif, transparan, dan berbasis bukti sehingga kualitas pengambilan keputusan dapat ditingkatkan secara lebih sistematis.

Implikasi lainnya adalah peluang integrasi model *Bayesian Network* ke dalam sistem informasi penanganan perkara yang telah digunakan oleh lembaga penegak hukum. Dengan mengintegrasikan variabel-variabel risiko ke dalam sistem digital, proses evaluasi perkara dapat dilakukan secara lebih cepat melalui simulasi berbagai skenario sebelum keputusan penuntutan diambil. Pendekatan tersebut tidak dimaksudkan untuk menggantikan diskresi jaksa, melainkan memberikan informasi tambahan yang dapat memperkuat pertimbangan profesional dalam menentukan strategi pembuktian. Oleh karena itu, model ini memiliki potensi untuk mendukung modernisasi tata kelola penuntutan sejalan dengan transformasi digital dalam sistem peradilan pidana.

Meskipun memberikan hasil yang menjanjikan, penelitian ini masih memiliki beberapa keterbatasan. Pertama, model yang dikembangkan menggunakan data simulasi sehingga distribusi probabilitas belum sepenuhnya merepresentasikan karakteristik perkara kejahatan siber yang terjadi dalam praktik. Kedua, struktur *Bayesian Network* dibangun berdasarkan hubungan konseptual antarvariabel sehingga masih memerlukan validasi empiris menggunakan data perkara aktual dari institusi penegak hukum. Ketiga, penelitian ini hanya mempertimbangkan sejumlah variabel utama yang berkaitan dengan pembuktian dan penuntutan, sementara faktor lain seperti kapasitas kelembagaan, beban perkara, dinamika persidangan, karakteristik hakim, serta perkembangan teknologi siber belum dimasukkan ke dalam model. Keterbatasan tersebut membuka peluang bagi penelitian selanjutnya untuk mengembangkan model yang lebih komprehensif dengan melibatkan data empiris dalam jumlah yang lebih besar, metode pembelajaran struktur jaringan secara otomatis (*structure learning*), maupun integrasi dengan teknik kecerdasan komputasional lainnya.

Dengan demikian, hasil penelitian menunjukkan bahwa pendekatan *Bayesian Network* memberikan perspektif baru dalam analisis penuntutan perkara kejahatan siber. Model yang dikembangkan tidak hanya menghasilkan estimasi probabilitas keberhasilan penuntutan, tetapi juga mampu menjelaskan hubungan kausal antar faktor pembuktian yang membentuk risiko secara keseluruhan. Kemampuan tersebut menjadikan *Bayesian Network* sebagai pendekatan yang relevan untuk mendukung pengembangan sistem penuntutan berbasis risiko, meningkatkan kualitas pengambilan keputusan, serta memperkuat efektivitas penegakan hukum terhadap kejahatan siber yang semakin kompleks.

IV. KESIMPULAN

Penelitian ini berhasil mengembangkan suatu arsitektur risiko penuntutan pada perkara kejahatan siber menggunakan pendekatan Bayesian Network yang mampu merepresentasikan hubungan probabilistik antar faktor pembuktian dalam proses penuntutan. Berbeda dengan pendekatan konvensional yang umumnya mengevaluasi setiap faktor secara terpisah, model yang dikembangkan menunjukkan bahwa keberhasilan penuntutan merupakan hasil interaksi berbagai variabel yang saling bergantung, meliputi kualitas bukti elektronik, integritas chain of custody, validitas prosedur penyitaan, kompetensi digital forensik, keberhasilan identifikasi pelaku, efektivitas kerja sama lintas yurisdiksi, serta kualitas konstruksi dakwaan. Hasil simulasi memperlihatkan bahwa kualitas bukti elektronik dan integritas chain of custody merupakan faktor yang memberikan kontribusi paling besar terhadap perubahan probabilitas keberhasilan penuntutan. Temuan tersebut menegaskan bahwa pendekatan probabilistik mampu memberikan gambaran yang lebih komprehensif mengenai mekanisme pembentukan risiko dibandingkan pendekatan linier, sekaligus mendukung proses evaluasi kesiapan pembuktian secara lebih objektif dan sistematis.

Kontribusi utama penelitian ini terletak pada pengembangan model risk-based prosecution berbasis Bayesian Network yang tidak hanya berfungsi sebagai alat estimasi probabilitas, tetapi juga sebagai kerangka analitis untuk mendukung pengambilan keputusan dalam penanganan perkara kejahatan

siber. Model yang dihasilkan berpotensi dimanfaatkan sebagai decision support system dalam membantu jaksa mengidentifikasi faktor-faktor kritis yang perlu diperkuat sebelum perkara dilimpahkan ke persidangan, sehingga strategi pembuktian dapat disusun secara lebih efektif dan berbasis bukti. Meskipun demikian, model yang dikembangkan masih memerlukan validasi menggunakan data perkara aktual agar tingkat akurasi probabilitas semakin meningkat. Oleh karena itu, penelitian selanjutnya disarankan mengintegrasikan data empiris dari perkara kejahatan siber yang telah diputus, menerapkan pembelajaran struktur jaringan (structure learning) maupun pembelajaran parameter (parameter learning), serta mengombinasikan Bayesian Network dengan teknik analitik lainnya untuk menghasilkan model penilaian risiko penuntutan yang lebih adaptif, akurat, dan aplikatif dalam mendukung modernisasi sistem peradilan pidana di era digital.

REFERENCES

Ahmed, S., Kaiser, M. S., Shahadat Hossain, M., & Andersson, K. (2025). A Comparative Analysis of LIME and SHAP Interpreters With Explainable ML-Based Diabetes Predictions. *IEEE Access*, *13*, 37370–37388. https://doi.org/10.1109/ACCESS.2024.3422319

Ali, M. G., Jasim, A. K., Shalaan, S. A. S. J., Jawad, H. M., Alsammarraie, R. M., & Iurynets, J. (2026). Cybercrime Legislation as a Catalyst for Digital Economic Growth: A Social Science Approach. *Communications in Computer and Information Science*, *2855 CCIS*, 19–40. https://doi.org/10.1007/978-3-032-17023-1_2

Allgaier, J., Mulansky, L., Draelos, R. L., & Pryss, R. (2023). How does the model make predictions? A systematic literature review on the explainability power of machine learning in healthcare. *Artificial Intelligence in Medicine*, *143*. https://doi.org/10.1016/j.artmed.2023.102616

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences*, *12*(11). https://doi.org/10.3390/socsci12110629

Carannante, M., & Mazzoccoli, A. (2025). An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective. *Risks*, *13*(8). https://doi.org/10.3390/risks13080144

Coelho, F., Rando, B., Aparício, D., Pontífice-Sousa, P., Gonçalves, D., & Abreu, A. M. (2026). The impact of educational gamification on cognition, emotions, and motivation: a randomized controlled trial. *Journal of Computers in Education*, *13*(2), 537–584. https://doi.org/10.1007/s40692-025-00366-x

Coupland, H. (2025). Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. *York Law Review*.

D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. *Healthcare (Switzerland)*, *11*(5). https://doi.org/10.3390/healthcare11050634

Datta, A., Sujay, D., & Shandilya, S. K. (2024). Introduction to Cyber Crime Investigation: A Modern Approach. *Advancements in Cyber Crime Investigations and Modern Data Analytics*, 1–15. https://doi.org/10.1201/9781003471103-1

Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, *7*(1).

https://doi.org/10.1002/spy2.333

Gulabivala, K., & Ng, Y. L. (2023). Factors that affect the outcomes of root canal treatment and retreatment—A reframing of the principles. *International Endodontic Journal*, *56*(S2), 82–115. https://doi.org/10.1111/iej.13897

Jaiswal, A., & Singh, S. (2025). Evolving Paradigms of Criminal Law in Contemporary India: Challenges, Reforms, and the Quest for Justice in a Digital Age. *LawFoyer International Journal of Doctrinal Legal Research*, *3*(1), 839–868. https://doi.org/10.70183/lijdlr.2024.v03.34

Krapu, C., Stewart, R., & Rose, A. (2023). A Review of Bayesian Networks for Spatial Data. *ACM Transactions on Spatial Algorithms and Systems*, *9*(1). https://doi.org/10.1145/3516523

Kwon, S. K., Seog, M., Kim, D., & Jung, I. Y. (2025). Impact of minimally invasive root canal treatment on healing outcomes in a randomized clinical trial. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-02905-z

Mokofe, W. M. (2023). Digital Transformations of the South African Legal Landscape. *Journal of Digital Technologies and Law*, *1*(4), 1087–1104. https://doi.org/10.21202/jdtl.2023.47

Morić, Z., Dakić, V., & Ogrizek Biškupić, I. (2026). An Empirical Assessment of Digital Forensic Process Reliability Using Integrated ISO/IEC 27037 and 27041 Standards. *Journal of Cybersecurity and Privacy*, *6*(2). https://doi.org/10.3390/jcp6020057

Mushtaq, S., & Shah, M. (2024). Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. *Information (Switzerland)*, *15*(10). https://doi.org/10.3390/info15100619

Nath, S., Summers, K., Baek, J., & Ahn, G. J. (2024). Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. *Proceedings - 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, TPS-ISA 2024*, 11–20. https://doi.org/10.1109/TPS-ISA62245.2024.00012

Ndibe, O. S. (2025). AI-Driven Forensic Systems for Real-Time Anomaly Detection and Threat Mitigation in Cybersecurity Infrastructures. *International Journal of Research Publication and Reviews*, *6*(5), 389–411. https://doi.org/10.55248/gengpi.6.0525.1991

Ni, Y., Baladandayuthapani, V., Vannucci, M., & Stingo, F. C. (2022). Bayesian graphical models for modern biological applications. *Statistical Methods and Applications*, *31*(2), 197–225. https://doi.org/10.1007/s10260-021-00572-8

Paul, J., Ueno, A., Dennis, C., Alamanos, E., Curtis, L., Foroudi, P., Kacprzak, A., Kunz, W. H., Liu, J., Marvi, R., Nair, S. L. S., Ozdemir, O., Pantano, E., Papadopoulos, T., Petit, O., Tyagi, S., & Wirtz, J. (2024). Digital transformation: A multidisciplinary perspective and future research agenda. *International Journal of Consumer Studies*, *48*(2). https://doi.org/10.1111/ijcs.13015

Sarker, I. H. (2023). Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*(6), 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Sestino, A., Kahlawi, A., & De Mauro, A. (2025). Decoding the data economy: a literature review of its impact on business, society and digital transformation. *European Journal of Innovation Management*, *28*(2), 298–323. https://doi.org/10.1108/EJIM-01-2023-0078

Sharma, S. (2024). Digital Forensics: Legal Standards and Practices in Cybercrime Investigation. *4th International Conference on Innovative Practices in Technology and Management 2024, ICIPTM 2024*. https://doi.org/10.1109/ICIPTM59628.2024.10563327

Sheoran, M. (2025). The Critical Role of Forensic Evidence in Modern Criminal Investigations.

International Journal of Law Management & Humanities, *8*(2), 2105–2133.

Singh, J. P., & Saxena, D. J. (2025). Navigating Cybercrime in India: Legal Complexities, Enforcement Dynamics, and Emerging Challenges in a Digitally Connected Society. *LawFoyer International Journal of Doctrinal Legal Research*, *3*(1), 650–681. https://doi.org/10.70183/lijdlr.2024.v03.27

Vogels, L., Mohammadi, R., Schoonhoven, M., & Birbil, İ. (2024). Bayesian Structure Learning in Undirected Gaussian Graphical Models: Literature Review with Empirical Comparison. *Journal of the American Statistical Association*, *119*(548), 3164–3182. https://doi.org/10.1080/01621459.2024.2395504

Wang, F., & Pei, W. (2026). Constructing Offender Typologies From Judicial Data: A Clustering Analysis of Sextortion Cases. *Sexual Abuse*. https://doi.org/10.1177/10790632261434143

Zhanbayev, R. A., Irfan, M., Shutaleva, A. V., Maksimov, D. G., Abdykadyrkyzy, R., & Filiz, Ş. (2023). Demoethical Model of Sustainable Development of Society: A Roadmap towards Digital Transformation. *Sustainability (Switzerland)*, *15*(16). https://doi.org/10.3390/su151612478

Zhang, A., Bradford, B., & Belur, J. (2026). Law-framed reasoning process: integrating mobile phone data in police investigations in China. *Policing and Society*. https://doi.org/10.1080/10439463.2026.2688971