Jurnal Pendidikan Sains dan Komputer

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Model Konseptual Arsitektur Pertahanan Diri Adaptif Berbasis RASP dan MAPE-K untuk Aplikasi Web

Nana Mulyana[1)*], Miswanto[2)], Rahmat Nursiaga[3)], Toni Saidun Ali[4)], Imam Santoso[5)]
[1)2)3)4)5)]Universitas Teknologi Muhammadiyah Jakarta, Indonesia
[1)]nana@utmj.ac.id [2)]miswanto@utmj.ac.id [3)]rahmat.nursiaga@utmj.ac.id [4)]toni@utmj.ac.id
[5)]imam.santoso@utmj.ac.id

***Nana Mulyana**

Histori Artikel:
Submit: 2025-10-18
Diterima: 2025-10-24
Dipublikasikan: 2025-10-27

Kata Kunci:
Analisis perilaku; Keamanan aplikasi adaptif; Keamanan otonom; Pembelajaran berkelanjutan; Umpan balik adaptif;

ABSTRAK

Keamanan aplikasi web modern menghadapi tantangan yang semakin kompleks karena munculnya serangan dinamis saat runtime. Mekanisme pertahanan tradisional seperti Web Application Firewall (WAF) dan Intrusion Detection System (IDS) terbatas karena hanya beroperasi secara statis di luar konteks aplikasi. Penelitian ini mengusulkan Model Konseptual Arsitektur Pertahanan Diri Runtime Adaptif yang mengintegrasikan Runtime Application Self-Protection (RASP), Behaviour Analysis, dan kerangka Monitor–Analyze–Plan–Execute over Knowledge (MAPE-K). Model ini dirancang untuk menciptakan sistem keamanan yang mampu memantau, menilai, dan menyesuaikan kebijakan pertahanan secara mandiri berdasarkan perilaku aktual aplikasi. Dengan pendekatan konseptual dan analisis teori sintetis, penelitian ini menghasilkan rancangan arsitektur pertahanan diri berbasis umpan balik adaptif (adaptive feedback loop). Arsitektur ini memungkinkan pengubahan data perilaku menjadi keputusan kontekstual, kemudian dievaluasi melalui Knowledge Base untuk pembelajaran berkelanjutan. Hasil analisis menunjukkan bahwa model ini memperluas konsep perlindungan aplikasi menuju kerangka keamanan otonom, di mana aspek keamanan menjadi tidak lagi reaktif, tetapi reflektif dan evolusioner. Secara praktis, model ini memberi dasar bagi pengembang aplikasi untuk membangun agen keamanan internal yang adaptif, serta bagi institusi keamanan siber dalam merancang platform otonom yang mampu belajar dari pola serangan aktual. Penelitian selanjutnya akan fokus pada pengujian empiris efektivitas model, pengembangan mekanisme meta-adaptif, dan aplikasi dalam lingkungan cloud multi-tenant untuk menilai skala dan stabilitas sistem pertahanan diri adaptif.

LATAR BELAKANG

Keamanan aplikasi web menjadi isu krusial dalam ekosistem digital modern karena sebagian besar serangan siber kini menargetkan lapisan aplikasi, bukan jaringan atau infrastruktur. Menurut Gartner, Inc. (2019), bahwa lebih dari dua pertiga serangan terhadap sistem informasi berasal dari kelemahan logika internal aplikasi yang dieksploitasi pada tingkat *runtime*. Ancaman seperti *webshell injection*, *file upload exploitation*, dan *command execution* menunjukkan bahwa penyerang semakin memanfaatkan kelemahan kontekstual saat aplikasi berjalan, bukan sekadar celah konfigurasional.

Pendekatan pertahanan tradisional seperti *Web Application Firewall (WAF)* dan *Intrusion Detection System (IDS)* telah banyak digunakan untuk mencegah eksploitasi tersebut. Namun, menurut laporan keamanan Check Point Software Technologies Ltd. (2022), mekanisme eksternal semacam ini bersifat statis dan hanya mampu mendeteksi pola serangan yang telah dikenali melalui tanda tangan (*signature-based detection*). Akibatnya, sistem ini kurang efektif menghadapi ancaman dinamis seperti *zero-day attacks* dan serangan polimorfik yang mengubah pola eksekusinya secara real time. Beberapa penelitian terbaru, seperti Li, Zhao, dan Sun (2020) melalui SunDEW Framework dan Contrast Security (2019) memperkenalkan konsep Runtime Application Self-Protection (RASP), sebuah mekanisme pertahanan tingkat aplikasi, tetapi masih bergantung pada agen eksternal atau konfigurasi statis

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

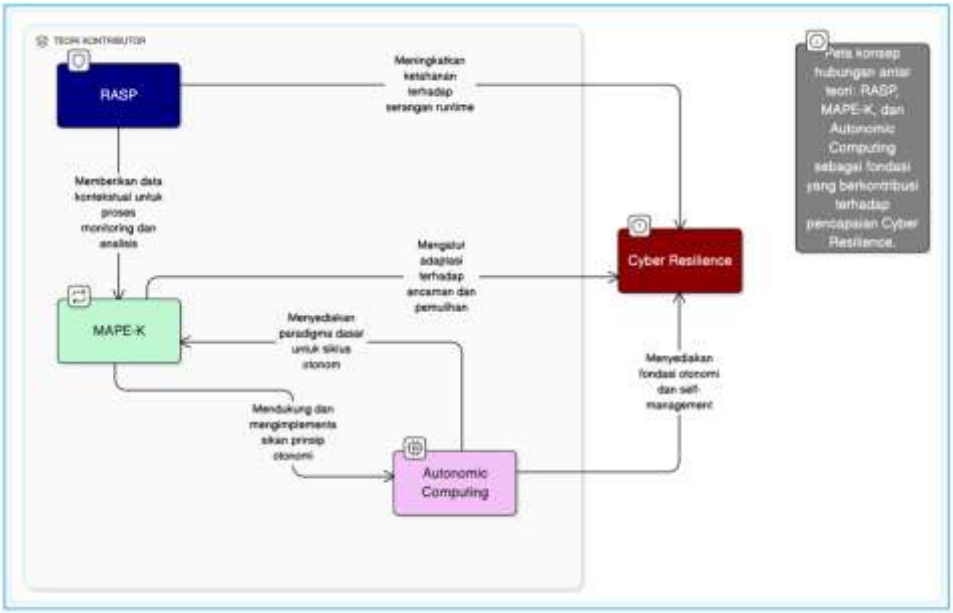
yang kurang adaptif terhadap kondisi runtime. Hingga saat ini, belum ada framework atau platform terbuka yang mengintegrasikan analisis perilaku, adaptivitas berbasis MAPE-K, dan otonomi pertahanan diri dalam satu arsitektur konseptual yang lengkap.

Penelitian ini merumuskan model konseptual arsitektur pertahanan diri runtime adaptif yang menggabungkan tiga landasan utama: (1) prinsip Runtime Application Self-Protection (RASP), (2) analisis perilaku berbasis deteksi anomali perilaku, dan (3) model adaptivitas MAPE-K (Monitor–Analyze–Plan–Execute over Knowledge). Model ini tidak hanya menampilkan mekanisme deteksi internal, tetapi juga menjadikan aplikasi sebagai entitas otonom yang mampu mengenali, menganalisis, dan memulihkan dirinya secara kontekstual terhadap ancaman. Dengan demikian, pendekatan ini memperluas batasan teori RASP konvensional menuju konsep baru: Adaptive RASP atau sistem pertahanan runtime otonom.

Untuk memperkuat dasar konseptual dari model yang diajukan, bagian ini membahas landasan teoretis yang mencakup prinsip Runtime Application Self-Protection (RASP) sebagai mekanisme keamanan internal aplikasi, pendekatan analisis perilaku untuk mendeteksi anomali aktivitas runtime, serta kerangka adaptivitas Monitor–Analyze–Plan–Execute over Knowledge (MAPE-K) yang mendasari sistem pertahanan otonom. Kajian literatur ini bertujuan menegaskan posisi penelitian dalam konteks perkembangan teori autonomic computing dan cyber resilience, sekaligus menunjukkan kontribusi konseptual terhadap arah baru keamanan aplikasi berbasis adaptivitas dan pembelajaran mandiri.

STUDI LITERATUR

Penelitian ini berlandaskan pada empat teori utama, yaitu *Runtime Application Self-Protection (RASP)*, *Monitor–Analyze–Plan–Execute over Knowledge (MAPE-K)*, *Autonomic Computing*, dan *Cyber Resilience*. Keempatnya saling melengkapi dan membentuk kerangka konseptual pertahanan diri runtime adaptif yang menjadi fokus penelitian. RASP menyediakan mekanisme perlindungan internal berbasis konteks, MAPE-K berfungsi sebagai siklus adaptasi otonom, *Autonomic Computing* memberikan prinsip kemandirian sistem, sedangkan *Cyber Resilience* menjadi tujuan akhir berupa kemampuan sistem untuk bertahan dan pulih dari ancaman. Untuk memperjelas hubungan antar teori, Gambar 1 menyajikan peta konsep sintesis yang menunjukkan bagaimana RASP, MAPE-K, dan *Autonomic Computing* berinteraksi serta berkontribusi terhadap terbentuknya *Cyber Resilience*.



Gambar 1. Peta Konsep Hubungan Antar Teori

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

RASP beroperasi dalam konteks eksekusi aplikasi dan berperan sebagai fondasi utama dalam sistem keamanan adaptif. Seperti yang dijelaskan oleh Gartner, Inc. (2019), RASP sebagai pendekatan keamanan yang tertanam langsung di dalam aplikasi (*in-app protection*), bukan pada lapisan eksternal seperti *Web Application Firewall (WAF)* atau *Intrusion Detection System (IDS)*. Pendekatan ini memungkinkan aplikasi memantau aktivitas internal, menganalisis perilaku pengguna, serta mencegah eksploitasi selama runtime berlangsung. Dengan visibilitas penuh terhadap logika bisnis dan aliran data, RASP memperluas paradigma keamanan dari berbasis perimeter menuju keamanan kontekstual yang beroperasi di tingkat eksekusi program. Pendekatan ini menandai pergeseran penting dari keamanan pasif menuju sistem yang memahami dirinya sendiri.

Implementasi RASP generasi pertama bersifat *rule-based* dan reaktif, bergantung pada agen eksternal pada tingkat framework. Banyak solusi komersial seperti Contrast Security dan Imperva RASP menggunakan aturan deteksi statis yang mirip sistem tanda tangan, membatasi kemampuan mereka untuk melawan serangan zero-day dan kode berbahaya yang menggunakan obfuscation atau morphing. Sistem RASP tradisional belum mengintegrasikan pembelajaran perilaku atau kemampuan adaptif, sehingga sulit menyesuaikan kebijakan keamanan saat kondisi runtime berubah. RASP konvensional masih beroperasi dalam paradigma pertahanan deterministik yang mengharuskan konfigurasi manual administrat.

Meskipun menjanjikan, berbagai penelitian menunjukkan bahwa implementasi RASP masih memiliki keterbatasan. Seperti dijelaskan oleh Contrast Security (2019), sebagian besar sistem RASP komersial bergantung pada aturan statis dan agen eksternal, sehingga cenderung bersifat reaktif terhadap ancaman baru. Li, Zhao, dan Sun (2020) mengembangkan Kerangka SunDEW yang memperluas RASP dengan agen analisis perilaku, tetapi sistem ini tetap kurang mampu beradaptasi terhadap perubahan konteks runtime.

Keterbatasan ini menciptakan kebutuhan akan lapisan kecerdasan tambahan yang mampu memahami pola perilaku aplikasi dan mengubahnya menjadi pengetahuan kontekstual bagi sistem keamanan. Dalam konteks ini, Analisis Perilaku muncul sebagai komponen penting yang menghubungkan RASP dan mekanisme adaptasi. Axelsson (2000) memperkenalkan pendekatan deteksi berbasis anomali sebagai dasar analisis perilaku, dengan menekankan pentingnya pemahaman terhadap perilaku dasar untuk mendeteksi aktivitas abnormal yang menyimpang dari pola operasi sistem. Prinsip ini kemudian dikembangkan lebih jauh oleh Mukkamala, Sung, dan Abraham (2003), yang menunjukkan bahwa model berbasis perilaku mampu mengenali serangan yang tidak terdeteksi oleh metode tanda tangan tradisional. Dalam konteks keamanan aplikasi, analisis perilaku berfungsi sebagai sensor cerdas yang memungkinkan sistem belajar dari interaksi nyata dan memperbarui persepsinya terhadap kondisi aman maupun bahaya berisiko.

Dengan mengintegrasikan analisis perilaku, sistem pertahanan diri tidak hanya mengandalkan deteksi pola statis seperti pada RASP konvensional, tetapi juga memperoleh kemampuan menginterpretasikan dinamika eksekusi secara adaptif. Garfinkel (2015) menegaskan bahwa pendekatan berbasis perilaku memperluas paradigma keamanan dari deteksi reaktif menjadi pemahaman proaktif, karena sistem mampu menghubungkan gejala perilaku dengan konteks ancaman yang lebih luas. Menurut Chandola, Banerjee, dan Kumar (2009), pendekatan berbasis perilaku memungkinkan sistem mengenali dinamika kompleks dalam eksekusi program melalui pengukuran entropi (ΔH) atau deviasi perilaku terhadap baseline. Analisis ini kemudian menjadi masukan penting untuk mekanisme penyesuaian kebijakan yang dijalankan oleh kerangka MAPE-K. Tanpa lapisan analisis perilaku, MAPE-K hanya bereaksi terhadap data mentah, bukan terhadap pemahaman kontekstual yang menunjukkan potensi ancaman secara lebih akurat.

Konsep Monitor–Analyze–Plan–Execute over Knowledge (MAPE-K), seperti yang dikemukakan oleh Kephart dan Chess (2003), menggambarkan mekanisme adaptasi otomatis melalui siklus reflektif yang terdiri dari empat komponen: Monitor, Analyze, Plan, dan Execute, semuanya bekerja di atas dasar pengetahuan. Dalam model ini, komponen Monitor berfungsi untuk memantau kondisi sistem, Analyze menilai anomali dan tren, Plan merancang strategi tindakan, dan Execute menjalankan keputusan berdasarkan konteks yang diperoleh. Kephart dan Chess (2003) menegaskan bahwa siklus ini merupakan inti dari autonomic computing yang memungkinkan sistem menyesuaikan

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

perilaku berdasarkan pengalaman dan data runtime. Dalam konteks keamanan aplikasi, mekanisme ini menciptakan sistem yang responsif dan berkesinambungan dalam mendeteksi serta menanggapi ancaman.

Nami dan Bertels (2007) menunjukkan bahwa MAPE-K efektif dalam meningkatkan kemampuan sistem beradaptasi terhadap perubahan lingkungan, sementara Villegas et al. (2011) menekankan peran pentingnya dalam memfasilitasi pengambilan keputusan otomatis berbasis feedback control loop. Namun, penerapan MAPE-K dalam keamanan runtime aplikasi masih jarang dan lebih banyak terbatas pada manajemen sumber daya. Selain itu, MAPE-K memiliki kelemahan inheren saat digunakan secara terisolasi. Tanpa data perilaku kontekstual dari RASP dan interpretasi kognitif dari Behaviour Analysis, proses adaptasinya berpotensi menghasilkan keputusan yang tidak relevan dengan kondisi runtime saat ini. Oleh karena itu, mengintegrasikan ketiga konsep ini menciptakan ekosistem yang adaptif, di mana RASP berfungsi sebagai sumber persepsi, Behaviour Analysis sebagai penafsir, dan MAPE-K sebagai pengendali kebijakan.

Prinsip adaptasi dalam MAPE-K sangat berkaitan dengan teori Autonomic Computing yang dikembangkan oleh IBM. Kephart dan Chess (2003) menjelaskan konsep ini melalui analogi sistem saraf otonom manusia yang mampu mengatur dirinya sendiri. Paradigma Autonomic Computing didasarkan pada empat pilar utama: self-configuration, self-optimization, self-healing, dan self-protection. Keempat kemampuan ini membuat sistem komputer menjadi entitas aktif yang bisa beradaptasi dan memperbaiki diri sesuai perubahan lingkungan dan kondisi internal. Pendekatan ini secara fundamental mengubah pandangan terhadap sistem komputer, dari yang semula pasif dan dikendalikan manusia, menjadi sistem cerdas yang mampu mengelola kompleksitasnya secara otomatis mandiri.

Dalam konteks keamanan aplikasi, prinsip self-healing dan self-protection dalam Autonomic Computing sangat relevan. Kephart dan Chess (2003) menegaskan bahwa sistem otonom harus mampu mengenali, merespons, dan memulihkan diri dari kesalahan tanpa intervensi manusia. Prinsip ini kemudian diperluas oleh penelitian terkini yang menyoroti pentingnya otonomi dalam keamanan sistem siber, di mana mekanisme pengambilan keputusan otomatis dianggap penting untuk menghadapi ancaman yang kompleks dan cepat berubah. Penelitian ini mengintegrasikan prinsip otonomi tersebut dengan menggabungkan Autonomic Computing ke dalam arsitektur pertahanan diri yang adaptif berbasis RASP dan MAPE-K. Melalui integrasi ini, sistem pertahanan tidak hanya bersifat reaktif, tetapi juga reflektif dan proaktif, mampu melakukan analisis situasi dan pembelajaran perilaku untuk meningkatkan ketahanan aplikasinya.

Landasan utama dari kerangka konseptual ini adalah Cyber Resilience, yang menempatkan tujuan keamanan bukan semata-mata pada pencegahan serangan, melainkan lebih pada kemampuan sistem untuk mempertahankan fungsi dan pulih dari gangguan. Linkov dan Trump (2019) menegaskan bahwa Cyber Resilience adalah kemampuan sistem digital untuk beradaptasi terhadap ancaman, menjaga stabilitas fungsional, dan melakukan pemulihan dengan dampak minimal. Paradigma ini memperluas definisi keamanan tradisional yang berfokus pada proteksi menjadi sistem yang menekankan keberlanjutan dan pembelajaran. Cyber Resilience tidak hanya menyoroti aspek pertahanan, tetapi juga menggabungkan dimensi adaptasi dan rekonstruksi sistem sebagai bagian dari strategi keamanan berkelanjutan.

Secara konseptual, keempat teori ini menempati tingkatan epistemik yang berbeda namun saling melengkapi. RASP bekerja pada domain persepsi teknis yang berfokus pada observasi perilaku, MAPE-K menyediakan mekanisme adaptasi berbasis siklus reflektif, Autonomic Computing memberikan dimensi kesadaran diri sistem, dan Cyber Resilience menambahkan orientasi jangka panjang pada kemampuan pemulihan. Dengan menghubungkan keempatnya, sistem pertahanan tidak hanya mampu mendeteksi dan merespons ancaman, tetapi juga mengevaluasi serta memperbaiki strategi perlindungan secara mandiri.

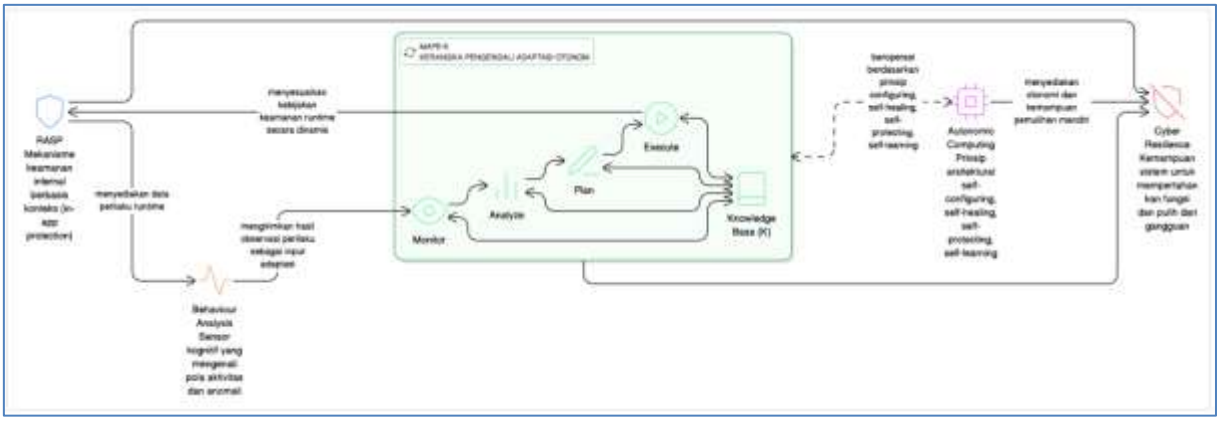
Secara kritis, literatur yang ada menunjukkan bahwa penelitian sebelumnya cenderung memisahkan fungsi deteksi, analisis, dan adaptasi. Kebanyakan studi RASP fokus pada peningkatan akurasi deteksi tanpa mekanisme adaptasi kebijakan, sementara pendekatan berbasis MAPE-K biasanya digunakan dalam manajemen sumber daya, bukan keamanan. Autonomic Computing banyak diterapkan dalam sistem terdistribusi, tetapi belum secara mendalam dalam konteks keamanan aplikasi web yang dinamis. Keterpisahan antara fungsi deteksi, analisis, dan adaptasi

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

menyebabkan sistem keamanan tetap berada pada paradigma reaktif. Padahal, dalam konteks ancaman dinamis, kemampuan untuk menafsirkan perilaku aplikasi dan menyesuaikan kebijakan secara real-time menjadi keharusan.

Kesenjangan tersebut menunjukkan bahwa tantangan keamanan modern tidak dapat diselesaikan dengan pendekatan tunggal. Literatur yang ada belum menempatkan integrasi antara persepsi runtime, interpretasi perilaku, dan adaptasi kebijakan sebagai satu kesatuan epistemik. Pendekatan konseptual yang diajukan dalam penelitian ini tidak hanya menggabungkan fungsi-fungsi tersebut, tetapi juga menyatukan logika persepsi (RASP), kognisi perilaku (Behaviour Analysis), dan refleksi adaptif (MAPE-K) dalam kerangka otonomi sistem yang bersifat belajar mandiri.

Kekosongan ini belum dijawab oleh penelitian sebelumnya dan menjadi dasar pengembangan model konseptual yang diusulkan. Oleh karena itu, penelitian ini mengisi kekosongan literatur dalam pengintegrasian teori adaptasi (MAPE-K) dengan mekanisme persepsi perilaku (RASP dan Behaviour Analysis) di bawah kerangka otonomi sistem (Autonomic Computing) untuk menciptakan Cyber Resilience yang adaptif terhadap kondisi runtime aplikasi web modern. Sintesis konseptual ini berbeda dari penelitian sebelumnya karena tidak hanya menggabungkan teori-teori yang ada, tetapi juga membangun hubungan fungsional dan epistemik antar lapisan persepsi, kognisi, adaptasi, dan ketahanan sebagai fondasi bagi sistem keamanan otonom yang reflektif. Berdasarkan sintesis hubungan antar teori tersebut, penelitian ini merumuskan model konseptual pertahanan diri runtime adaptif sebagaimana divisualisasikan pada Gambar 2 yang pembahasannya akan dibahas lebih lanjut di bagian hasil dan pembahasan. Dengan demikian, studi ini tidak hanya memperluas batas konseptual RASP dan MAPE-K, tetapi juga menawarkan sintesis baru bagi penelitian keamanan otonom berbasis perilaku runtime.



Gambar 2. Model konseptual pertahanan diri runtime adaptif

Berdasarkan sintesis teori-teori yang telah dibahas, penelitian ini mengajukan sebuah model konseptual arsitektur pertahanan diri runtime adaptif. Model ini mengintegrasikan mekanisme *Runtime Application Self-Protection (RASP)*, analisis perilaku sebagai sensor kognitif, dan kerangka adaptasi otonom *MAPE-K* di bawah prinsip *Autonomic Computing* untuk mencapai *Cyber Resilience*. Hubungan antar komponen utama model konseptual tersebut divisualisasikan pada Gambar 2. Model konseptual pertahanan diri runtime adaptif yang diusulkan inilah yang menjadi kontribusi utama penelitian dan akan dijelaskan lebih lanjut pada bagian hasil penelitian.

METODE

Penelitian ini menggunakan pendekatan studi pustaka sebagai metode utama. Alasan dipilihnya studi pustaka adalah karena fokus penelitian adalah pengembangan model konseptual melalui analisis teori, sintesis kerangka pikir, dan perbandingan antar konsep dalam bidang keamanan aplikasi web modern. Menurut Mary W. George (2008), studi pustaka adalah proses sistematis untuk mengidentifikasi, mengevaluasi, dan menafsirkan berbagai sumber ilmiah guna membentuk pemahaman teoritis yang mendalam. Data dikumpulkan melalui penelusuran buku akademik, artikel jurnal nasional dan internasional yang bereputasi, serta laporan penelitian terkait Runtime Application Self-Protection

Jurnal Pendidikan Sains dan Komputer
Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

(RASP), sistem adaptif MAPE-K, analisis perilaku, dan keamanan siber autonomic frameworks.

Validitas konseptual dalam penelitian ini dijamin melalui triangulasi sumber, membandingkan ide, prinsip, dan temuan dari berbagai literatur nasional maupun internasional, termasuk whitepaper industri keamanan siber dan publikasi akademik di bidang autonomic computing dan cyber resilience. Adaptasi langkah-langkah George yang dimodifikasi meliputi: 1) Menetapkan topik penelitian tentang arsitektur pertahanan diri runtime adaptif untuk aplikasi web, 2) Merumuskan pertanyaan utama: "Bagaimana prinsip RASP, analisis perilaku, dan MAPE-K dapat diintegrasikan dalam satu model pertahanan diri yang adaptif ?", 3) Menentukan teori dasar: teori Runtime Application Self-Protection (RASP), Autonomic Computing, dan MAPE-K Adaptivity Model, 4) Menelusuri literatur pendukung dari jurnal nasional, internasional, serta laporan industri keamanan siber, 5) Mengidentifikasi kekurangan teoretis dari penelitian terdahulu, 6) Mengevaluasi sumber dan keabsahan literatur untuk memastikan kredibilitas referensi, 7) Menyusun dan merumuskan model konseptual arsitektur pertahanan diri runtime adaptif berdasarkan hasil sintesis, dan 8) Menarik kesimpulan bahwa integrasi RASP, analisis perilaku, dan MAPE-K mampu menciptakan paradigma baru dalam keamanan aplikasi yang berbasis adaptivitas dan otonomi sistem. Dengan demikian, metode penelitian ini bersifat **deskriptif-analitis dan konseptual**, berorientasi pada pengembangan teori, bukan pada pengujian empiris, serta berfungsi sebagai dasar untuk penelitian eksperimental lanjutan dalam domain keamanan aplikasi adaptif.

HASIL

Bagian ini menampilkan hasil rancangan model arsitektur pertahanan diri runtime adaptif yang dikembangkan dengan mengintegrasikan teori RASP, Behaviour Analysis, MAPE-K, dan Autonomic Computing. Karena ini adalah studi konseptual, fokusnya adalah pada struktur arsitektur, hubungan antar komponen, serta justifikasi teoretis dan fungsional dari setiap modul, tanpa melibatkan hasil empiris atau pengujian eksperimental. Tujuan utama dari rancangan ini adalah menciptakan fondasi untuk sistem keamanan aplikasi yang mampu menilai dan menyesuaikan kebijakan secara otomatis berdasarkan perilaku nyata aplikasi saat runtime.

Berdasarkan hasil sintesis teori yang dijelaskan dalam bagian Studi Literatur, hubungan antar teori utama divisualisasikan dalam Gambar 2. Gambar tersebut menunjukkan peran RASP sebagai mekanisme deteksi internal, Behaviour Analysis sebagai sensor kognitif yang mengenali pola aktivitas, MAPE-K sebagai kerangka kerja adaptasi otonom, Autonomic Computing sebagai prinsip pengendalian diri, dan Cyber Resilience sebagai hasil akhir dari seluruh integrasi tersebut. Model konseptual ini menjadi dasar untuk merancang arsitektur sistem yang diusulkan, sebagaimana ditunjukkan dalam Gambar 3. Diagram ini memperlihatkan implementasi konseptual hubungan teori-teori tersebut dalam bentuk arsitektur fungsional yang menampilkan komponen utama, aliran data, dan mekanisme feedback loop adaptif.

Gambar 3 menunjukkan arsitektur pertahanan diri runtime adaptif yang terdiri dari lima lapisan utama: *Runtime Monitoring Layer, Behaviour Analysis Layer, Decision and Response Layer, Knowledge Base, dan Adaptive Feedback Loop*. Model ini dirancang untuk mewakili aliran informasi dan umpan balik adaptif selama siklus eksekusi aplikasi. Setiap lapisan memiliki fungsi dan parameter konseptual yang mendukung mekanisme otonomi keamanan (autonomic self-protection).

Gambar 3. Arsitektur Pertahanan Diri Runtime Adaptif

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Proses dimulai dari **input pengguna (user input)** yang menjadi titik awal untuk setiap eksekusi sistem. Setiap interaksi pengguna, baik permintaan data, pengisian formulir, maupun aktivitas lain dalam aplikasi dengan berbagai metode *http* seperti *GET, POST, REQUEST, DELETE,* atau *PUT* diterima sebagai sumber informasi utama yang akan dipantau. Pada tahap ini, sistem belum mengambil keputusan terkait keamanan, tetapi memastikan bahwa setiap input dikemas dalam konteks eksekusi lengkap, termasuk data sesi, identitas pengguna, dan konteks fungsi yang sedang berjalan. Informasi kontekstual ini penting karena menjadi landasan untuk tahap pemantauan berikutnya dalam menilai apakah aktivitas termasuk perilaku normal atau berpotensi berbahaya ancaman.

Langkah selanjutnya adalah **Layer Pemantauan Runtime (*Runtime Monitoring Layer*).** Lapisan ini berfungsi sebagai indera penglihatan sistem, memantau setiap aktivitas aplikasi selama proses berjalan. Di sini, sistem mengawasi validasi input, mencatat pemanggilan API (API Call) Log, dan memonitor fungsi berisiko tinggi seperti akses file, perintah sistem, atau manipulasi data sensitif. Tujuan utamanya bukan untuk menghentikan aktivitas, tetapi untuk mengumpulkan data perilaku secara kontekstual agar sistem dapat memahami apa yang terjadi di dalam aplikasi secara lengkap. Data dari hasil pemantauan, berupa log eksekusi dan konteksnya (misalnya jenis operasi, urutan eksekusi, dan status keberhasilan fungsi), dikirim secara terus-menerus ke Lapisan Analisis Perilaku **(***Behaviour Analysis Layer*) melalui mekanisme aliran data berbasis peristiwa.

Data hasil pemantauan runtime dianalisis oleh Lapisan Analisis Perilaku (Behaviour Analysis Layer), yang berfungsi sebagai sensor kognitif untuk mengenali pola aktivitas normal dan mendeteksi anomali menggunakan dua pendekatan: detection berbasis tanda untuk serangan dengan pola yang telah diketahui dan detection berbasis anomali untuk pola aktivitas baru yang belum dikenal. Secara konseptual, ΔH menunjukkan tingkat ketidakteraturan pola eksekusi fungsi dibandingkan baseline normal yang tersimpan dalam Knowledge Base. Jika ΔH melebihi ambang adaptif (Θ), sistem akan menandai aktivitas tersebut sebagai anomali potensial dan mengirimkan sinyal ke Decision and Response Layer. Mekanisme ini membangun hubungan parametrik antara lapisan analisis dan pengambilan keputusan, di mana ΔH dan Θ berfungsi sebagai indikator kuantitatif untuk proses tersebut adaptasi.

Hasil evaluasi dari lapisan analisis perilaku selanjutnya dikirim ke Lapisan Keputusan dan Respons (Decision & Response Layer). Lapisan ini berperan utama dalam menetapkan strategi adaptasi sistem berdasarkan hasil analisis anomali sebelumnya. Di sini diterapkan prinsip Monitor–Analyze–Plan–Execute over Knowledge (MAPE-K). Keputusan adaptif dibuat dengan membentuk policy vector yang mencakup tiga dimensi konsep: status kebijakan (aktif/nonaktif), tingkat risiko (r), dan prioritas respons (p). Hubungan antarvariabel dalam proses adaptasi dapat dinyatakan sebagai fungsi $f(\Delta H, \Theta, r, p)$, di mana perubahan nilai entropi (ΔH) dibandingkan dengan ambang adaptif (Θ) menentukan penyesuaian tingkat risiko (r) dan prioritas respons (p). Jika $\Delta H > \Theta$, maka nilai r ditingkatkan dan kebijakan p diperbarui melalui prosedur plan–execute untuk menyesuaikan tingkat perlindungan. Siklus ini berlangsung secara semi-kontinu dan terhubung langsung dengan Knowledge Base untuk memantau efektivitas kebijakan yang diterapkan.

Semua hasil keputusan dan evaluasi disimpan dalam Basis Pengetahuan (Knowledge Base), yang berfungsi sebagai memori adaptif untuk menyimpan pola perilaku, kebijakan yang pernah diterapkan, serta respons terhadap serangan. Komponen ini juga menyediakan konteks pengetahuan yang digunakan oleh lapisan lain dalam pengambilan keputusan. Secara konsep, Knowledge Base mendukung prinsip belajar mandiri, di mana sistem tidak hanya meniru kebijakan lama tetapi juga memperbaruinya berdasarkan evaluasi historis. Data kebijakan yang menunjukkan efektivitas tinggi diprioritaskan sebagai kebijakan utama, sementara kebijakan yang gagal menurunkan ΔH akan diperbarui atau dinonaktifkan secara otomatis. Proses ini menciptakan hubungan reflektif dua arah antara lapisan Decision and Response dan Runtime Monitoring, di mana sistem terus mengukur dampak kebijakan terhadap stabilitas perilaku aplikasi.

Hubungan antar modul dalam arsitektur ini bersifat **parametrik, iterative dan reflektif**, bukan hanya deskriptif. Data perilaku dari lapisan pemantauan menghasilkan nilai ΔH yang dibandingkan dengan Θ di lapisan analisis. Nilai ΔH yang melampaui Θ memicu pembaruan *policy vector* di lapisan keputusan. Setelah kebijakan baru diterapkan, perubahan perilaku berikutnya akan menghasilkan ΔH baru yang dievaluasi ulang, sehingga membentuk

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

siklus *adaptive feedback loop* yang bersifat self-regulating. Siklus ini memastikan sistem selalu beroperasi dalam keseimbangan antara stabilitas dan adaptasi terhadap ancaman baru, sesuai prinsip *autonomic computing*.

Secara konsep, hubungan antara Gambar 1 dan Gambar 2 menunjukkan proses mengubah kerangka teori menjadi arsitektur implementasi. Pada tingkat ini, Gambar 2 menampilkan penggabungan lima teori utama yang mendasari desain, di mana RASP dan Behaviour Analysis mewakili lapisan persepsi dan deteksi kontekstual, MAPE-K berfungsi sebagai mekanisme adaptasi, Autonomic Computing menyumbang prinsip otonomi, dan Cyber Resilience menjadi tujuan akhir untuk ketahanan sistem yang berkelanjutan. Peralihan dari konsep ke arsitektur, digambarkan pada Gambar 3, menunjukkan bagaimana teori-teori tersebut dioperasionalkan: lapisan pemantauan dan analisis perilaku menerapkan prinsip RASP dan Behaviour Analysis, sedangkan Decision & Response Layer menerapkan MAPE-K yang menyesuaikan kebijakan keamanan runtime berdasarkan konteks yang diamati. Prinsip Autonomic Computing diinternalisasi melalui mekanisme self-managing dan self-adapting, diwujudkan dalam pembaruan otomatis kebijakan dan self-recovery terhadap anomali yang terdeteksi. Seluruh proses ini bertujuan mencapai Cyber Resilience. Secara fungsional, arsitektur ini memiliki tiga kemampuan utama yang membedakannya dari model keamanan tradisional. Pertama, kemampuan deteksi kontekstual, di mana sistem memahami konteks eksekusi aplikasi, bukan hanya pola lalu lintas jaringan seperti pada WAF. Kedua, kemampuan adaptasi dinamis, yang memungkinkan sistem menyesuaikan kebijakan keamanan berdasarkan hasil analisis perilaku aktual. Ketiga, kemampuan pembelajaran berkelanjutan, diperoleh melalui mekanisme umpan balik berbasis Knowledge Base. Ketiga kemampuan ini menciptakan sistem pertahanan diri yang bersifat kontekstual, berbasis perilaku, dan secara otonom adaptive.

Dari segi perbandingan, model ini unggul secara konseptual dibandingkan pendekatan-pendekatan yang telah dikembangkan sebelumnya. Sebagai contoh, menurut Li, Zhao, dan Sun (2020), SunDEW Framework memperkenalkan agen eksternal berbasis analisis perilaku, meskipun tetap bergantung pada konfigurasi statis. Sebagaimana dijelaskan oleh Contrast Security (2019), Hybrid Application Shield hanya menambah fitur RASP melalui modul pelaporan, tanpa mekanisme pembelajaran adaptif. Berbeda dari kedua pendekatan tersebut, model dalam penelitian ini menggabungkan analisis perilaku runtime dan kebijakan adaptif berbasis MAPE-K dalam satu sistem otonom yang terintegrasi langsung dalam aplikasi. Dengan demikian, sistem ini tidak hanya mampu mendeteksi ancaman, tetapi juga belajar dari pola interaksi sebelumnya untuk meningkatkan kebijakan pertahanan.

Potensi penerapan model ini cukup tinggi karena semua komponennya dapat diintegrasikan ke dalam lingkungan aplikasi nyata. Runtime Monitoring dapat direalisasikan melalui agen instrumentation yang tertanam dalam aplikasi berbasis Java atau Python. Sementara itu, Behaviour Analysis Layer dapat menggunakan algoritma deteksi anomali urutan dan analisis deviasi berbasis entropi yang berfungsi secara real-time. Decision and Response Layer berperan sebagai modul kebijakan dinamis yang menyesuaikan parameter keamanan sesuai tingkat ancaman. Pada tahap berikutnya, variabel konseptual seperti ΔH (entropi perilaku), policy vectors, dan adaptive thresholds (Θ) dapat diubah menjadi variabel terukur untuk simulasi atau eksperimen. Dengan demikian, penelitian ini tidak hanya menawarkan model ideal secara teoritis, tetapi juga menyediakan kerangka operasional yang siap diuji untuk pengembangan sistem keamanan otonom berbasis adaptasi perilaku.

PEMBAHASAN

Berdasarkan hasil perancangan dan penjabaran arsitektur pertahanan diri runtime adaptif yang telah dijelaskan sebelumnya, dibutuhkan analisis lebih mendalam untuk memahami makna konseptual dan dampaknya. Pembahasan ini tidak hanya mengevaluasi kesesuaian hasil model dengan teori-teori dasar pengembangannya, tetapi juga meneliti sejauh mana model ini memperluas, menantang, atau mengubah pemahaman yang ada tentang sistem keamanan aplikasi berbasis otonomi. Oleh karena itu, bagian ini menitikberatkan pada analisis kritis dan reflektif terhadap model konseptual yang diajukan, baik dari sudut pandang teoretis maupun kontribusinya terhadap pengembangan paradigma pertahanan adaptif runtime.

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Model arsitektur pertahanan diri runtime adaptif menunjukkan pergeseran dari keamanan berbasis perimeter ke keamanan berbasis kesadaran kontekstual dan kemampuan penyesuaian internal. Dalam praktik keamanan tradisional, sistem umumnya bergantung pada mekanisme eksternal seperti Web Application Firewall (WAF) atau Intrusion Detection System (IDS), yang mendeteksi ancaman berdasarkan pola tanda tangan statis. Hasil rancangan model ini menunjukkan bahwa pendekatan tersebut tidak lagi memadai dalam menghadapi ancaman modern yang bersifat dinamis dan kontekstual di tingkat eksekusi aplikasi. Arsitektur yang diusulkan menempatkan mekanisme pertahanan langsung di dalam lingkungan eksekusi (pertahanan dalam aplikasi), sehingga keamanan menjadi fungsi internal yang mampu menilai kondisi aktual sistem dan menyesuaikan kebijakan secara adaptif. Dengan demikian, keamanan tidak lagi menjadi entitas pasif yang menunggu serangan, melainkan mekanisme aktif yang bereaksi dan berkembang bersama sistem.

Integrasi RASP, Behaviour Analysis, dan MAPE-K dalam model menunjukkan bahwa keamanan merupakan proses reflektif yang berputar secara siklik. Mekanisme feedback loop adaptif dalam model ini memperlihatkan bagaimana data perilaku yang dikumpulkan dari lapisan pemantauan dapat diubah menjadi pemahaman situasional di lapisan analisis, kemudian diterjemahkan menjadi keputusan adaptif di lapisan respons. Siklus ini menandai munculnya kecerdasan sistemik yang bersifat experiential, di mana sistem bukan hanya menjalankan kebijakan, tetapi juga belajar dari pengalaman interaksi sebelumnya. Proses ini memperluas konsep teori RASP klasik, yang sebelumnya hanya menekankan deteksi deterministik berbasis aturan. Dalam model ini, RASP berkembang menjadi sistem reflektif dan evolusioner yang mampu menyesuaikan kebijakan pertahanan secara kontekstual melalui mekanisme pembelajaran berbasis pengalaman runtime.

Dari sudut pandang analisis perilaku, hasil rancangan model menunjukkan bahwa Lapisan Analisis Perilaku mempunyai peran penting sebagai jembatan kognitif antara persepsi sistem dan tindakan adaptif. Lapisan ini bukan hanya komponen analitik, tetapi juga mekanisme epistemik yang memungkinkan sistem memahami dirinya melalui interpretasi perilaku. Dengan mengenali pola normal dan anomali secara kontekstual, sistem mengembangkan kemampuan "penilaian situasional" yang menyerupai fungsi kognitif manusia dalam pengambilan keputusan berbasis pengalaman. Secara reflektif, ini menunjukkan bahwa kecerdasan keamanan tidak lagi bergantung pada aturan eksplisit yang dirancang manusia, melainkan dari kemampuan sistem untuk menggeneralisasi dan menafsirkan perilaku. Fenomena ini mengindikasikan bahwa keamanan dapat bersifat emergen — muncul dari dinamika interaksi data dan konteks, bukan dari desain statis. Hal ini memperluas batas teori *computing autonomic* menuju ke ranah autonomic cognition, dimana sistem tidak hanya mengatur dirinya sendiri, tetapi juga membangun makna dari perilaku tersebut diamatinya.

Secara operasional, efektivitas model dapat diuji melalui pendekatan simulatif berbasis data runtime aplikasi. Variabel seperti entropi perilaku (ΔH), ambang adaptif (Θ), dan vektor kebijakan (p) digunakan untuk menilai stabilitas sistem terhadap perubahan perilaku pengguna maupun serangan dinamis. Peningkatan ΔH yang melebihi nilai Θ menunjukkan adanya anomali yang memicu modul adaptasi MAPE-K. Evaluasi keberhasilan kebijakan dilakukan dengan membandingkan nilai ΔH sebelum dan sesudah proses adaptasi. Dengan mekanisme ini, model dapat diuji secara empiris untuk menilai kemampuan mempertahankan kestabilan dan efektivitas kebijakan pertahanan di kondisi lingkungan yang berubah. Diharapkan, setelah proses adaptasi, nilai ΔH akan menurun, yang menandakan peningkatan stabilitas sistem dan efektivitas mekanisme pertahanan diri yang bersifat adaptif. Namun, efektivitas pendekatan ini tetap perlu diverifikasi melalui simulasi di berbagai konteks aplikasi dan beban kerja yang berbeda guna menilai tingkat generalisasi dan keandalan model secara lebih komprehensif.

Integrasi siklus Monitor–Analyze–Plan–Execute (MAPE-K) ke dalam arsitektur menambahkan dimensi reflektif terhadap proses adaptasi. Dalam konteks RASP konvensional, pengambilan keputusan berhenti pada deteksi dan mitigasi; sementara dalam model ini, proses dilanjutkan hingga evaluasi hasil keputusan dan pembaruan kebijakan melalui Knowledge Base. Secara konseptual, ini menandai pergeseran dari logika pelaksanaan aturan menuju pembelajaran melalui pengalaman. Sistem tidak hanya menjalankan kebijakan, tetapi juga menilai efektivitasnya dan memanfaatkannya untuk meningkatkan kebijakan selanjutnya. Dengan demikian, model ini menampilkan bentuk meta-adaptasi, di mana sistem tidak hanya beradaptasi terhadap lingkungan, tetapi juga terhadap metode beradaptasi.

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Proses pembelajaran berlapis ini membuat model lebih tahan terhadap kesalahan adaptasi dan lebih cerdas dalam merespons ancaman berubah-ubah.

Analisis hubungan antar lapisan dalam hasil model juga menunjukkan adanya keterpaduan antara fungsi teknis dan implikasi konseptual. Lapisan pemantauan runtime berfungsi sebagai sensor persepsi, lapisan analisis perilaku sebagai sistem penalaran kognitif, dan lapisan keputusan adaptif sebagai mekanisme refleksi. Hubungan ini membentuk struktur kesadaran buatan yang memungkinkan sistem melakukan introspeksi terhadap tindakannya sendiri. Secara teoretis, fenomena ini dapat dipahami sebagai bentuk computational self-awareness, di mana sistem mampu merepresentasikan dan menilai kondisi internalnya. Inilah dasar dari keamanan otonomik, yaitu keadaan di mana keamanan tidak lagi bergantung pada intervensi eksternal, melainkan muncul dari proses berpikir sistemik yang berkelanjutan.

Dari sudut pandang reflektif, hasil model ini juga menampilkan transformasi konseptual dari cyber resilience sebagai kondisi bertahan menjadi resilience sebagai proses. Saat sistem menghadapi serangan, tiga proses utama berlangsung: persepsi ancaman, penyesuaian kebijakan, dan regenerasi pengetahuan. Ketiganya menciptakan mekanisme pembelajaran yang berkelanjutan, di mana setiap gangguan tidak lagi dianggap sebagai kegagalan, melainkan sebagai pengalaman yang memperkuat kemampuan adaptasi sistem. Dengan demikian, ketahanan siber tidak lagi dipahami hanya sebagai kemampuan bertahan dari serangan, tetapi sebagai kemampuan berkembang melalui serangan. Ini menjadikan model yang diusulkan bukan sekadar arsitektur teknis, tetapi sebagai kerangka konseptual yang menegaskan bahwa keamanan sejati bersifat reflektif dan evolusioner.

Meskipun mekanisme self-learning dan adaptive feedback loop menawarkan fleksibilitas tinggi dalam menanggapi dinamika ancaman, tetapi keberhasilannya sangat bergantung pada dua faktor utama: keakuratan data perilaku yang dikumpulkan dan kemampuan sistem membedakan antara penyimpangan berbahaya dan perubahan normal. Ketergantungan pada data yang valid membuat model ini rentan terhadap bias persepsi jika data runtime yang diamati tidak mewakili kondisi aktual aplikasi. Refleksi kritis terhadap keterbatasan ini penting untuk menentukan batas operasional model dan menjadi dasar pengembangan lebih lanjut berikutnya.

Salah satu tantangan utama yang perlu diantisipasi adalah risiko false adaptation, yaitu saat sistem menyesuaikan kebijakan secara salah karena salah memahami pola perilaku. Risiko ini bisa meningkat jika model pembelajaran tidak memiliki mekanisme validasi kontekstual yang ketat terhadap sumber data dan pola serangan. Selain itu, mengintegrasikan lapisan pemantauan dan analisis perilaku berpotensi menambah beban komputasi, terutama pada aplikasi dengan volume data runtime besar dan frekuensi adaptasi tinggi. Kompleksitas ini dapat mempengaruhi performa sistem dan menyebabkan penundaan dalam pengambilan keputusan adaptif.

Ketergantungan pada sumber data perilaku yang akurat juga menjadi risiko, terutama ketika data terkontaminasi atau dimanipulasi melalui serangan poisoned telemetry. Dalam hal ini, lapisan kontrol meta-adaptive diperlukan untuk memverifikasi keandalan pengetahuan sebelum kebijakan baru diimplementasikan. Mekanisme ini berfungsi sebagai pengendali kesadaran sistem (meta-cognitive control) agar proses adaptasi tetap stabil dan tidak menimbulkan gangguan berantai. Dengan begitu, keseimbangan antara adaptivitas dan stabilitas hanya tercapai jika sistem mampu melakukan refleksi untuk menilai validitas pengetahuannya secara mandiri. Ke depan, penelitian lebih jauh harus difokuskan pada penguatan kapasitas kontrol meta-kognitif sebagai fondasi penting untuk mengembangkan kecerdasan otonom yang lebih andal, aman, dan kontekstual.

Secara umum, refleksi terhadap model arsitektur pertahanan diri runtime adaptif menunjukkan bahwa keamanan aplikasi dapat berkembang menjadi entitas yang mampu persepsi, belajar, dan beradaptasi secara mandiri. Model ini memperluas konsep RASP dengan menambahkan aspek kognitif dan reflektif, sekaligus menegaskan posisi pengolahan otomatis sebagai dasar keamanan autonomic. Temuan ini menegaskan kontribusi penelitian dalam memperluas konsep perlindungan aplikasi secara real-time menuju kerangka cybersecurity autonomic yang adaptif, reflektif, dan berkelanjutan. Berdasarkan dasar tersebut, bagian berikut menyajikan kesimpulan penelitian yang merangkum kontribusi utama, keterbatasan, serta arahan pengembangan model untuk penelitian selanjutnya mendatang.

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Dengan demikian, meskipun pembahasan ini disusun secara konseptual, model arsitektur yang diajukan memiliki arah empiris yang jelas dan dapat dievaluasi melalui simulasi perilaku runtime. Analisis terhadap potensi kelemahan model justru menjadi dasar penting untuk penyempurnaan desain adaptif dan pengujian sistem di tahap penelitian selanjutnya

KESIMPULAN

Penelitian ini mengusulkan model konseptual pertahanan diri runtime adaptif yang mengintegrasikan analisis perilaku, mekanisme MAPE-K, dan prinsip RASP sebagai pendekatan keamanan otonom berbasis konteks. Pendekatan ini menandai pergeseran paradigma dari keamanan reaktif menuju keamanan yang proaktif dan evolusioner di mana sistem tidak hanya melindungi diri dari ancaman, tetapi juga belajar dari perilaku dan pengalaman serangan.

Secara praktis, model ini memberikan dasar bagi pengembangan sistem keamanan yang adaptif dan efisien sumber daya melalui integrasi agen pemantauan dalam aplikasi tanpa ketergantungan pada sistem eksternal. Dengan begitu, penelitian ini berpotensi diterapkan dalam membangun sistem keamanan yang lebih real-time, dan tahan terhadap ancaman zero-day. Namun, efektivitasnya masih perlu diverifikasi secara empiris. Risiko *false adaptation*, *overhead* komputasi, serta ketergantungan terhadap keandalan data perilaku menjadi batasan utama yang perlu dikaji lebih lanjut.

Arah penelitian berikutnya bisa difokuskan pada pengujian empiris untuk menilai keefektifan model dalam berbagai skenario serangan aplikasi web. Selain itu, penelitian selanjutnya juga dapat mengembangkan mekanisme meta-adaptif yang mampu memverifikasi keabsahan keputusan adaptif dan mengelola risiko overfitting pada kebijakan keamanan. Penerapan model ini dalam platform keamanan berbasis otonomi terdistribusi atau lingkungan cloud multi-tenant merupakan arah yang potensial, guna mengevaluasi bagaimana prinsip pertahanan diri dapat diterapkan secara kolaboratif antar berbagai sistem. Dengan demikian, penelitian ini berkontribusi dalam memperluas konsep RASP menuju paradigma keamanan otonom, di mana sistem tidak sekadar terlindungi, tetapi juga mampu memahami dan mempertahankan integritasnya secara mandiri.

REFERENSI

Ashby, W. R. (1956). *An introduction to cybernetics*. Chapman & Hall.

Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy*. Chalmers University of Technology.

Check Point Software Technologies Ltd. (2022). *Runtime application self-protection (RASP): Principles and benefits*. Check Point Software Technologies.

Check Point Software Technologies Ltd. (2022). *Security report 2022: Cyber attack trends*. Check Point Research

Contrast Security. (2019). *RASP architectural overview and use cases*. Contrast Security.

Garfinkel, S. (2015). *The computer security handbook* (6th ed.). Wiley.

George, M. W. (2008). *The elements of library research: What every student needs to know*. Princeton University Press.

Gartner, Inc. (2019). *Emerging technology analysis: Runtime application self-protection*. Gartner Research.

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer, 36*(1), 41–50. https://doi.org/10.1109/MC.2003.1160055.

Li, J., Zhao, W., & Sun, D. (2020). SunDEW: A self-defense framework for web applications. In *Proceedings of the International Conference on Software Security and Assurance (ICSSA 2020)*.

Jurnal Pendidikan Sains dan Komputer
Volume 5, Number 02, Oktober 2025
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v5i02.7096

Li, S., Zhang, T., & Wang, X. (2024). A behavior-based anomaly detection framework for webshell identification. *Computers & Security, 118,* 102741

Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*. Springer. https://doi.org/10.1007/978-3-030-04565-4.

Mary, W. (2008). *The elements of library research*. Princeton University Press.

Mukkamala, S., Sung, A. H., & Abraham, A. (2003). Intrusion detection using an ensemble of intelligent paradigms. *Journal of Network and Computer Applications, 26*(2), 167–182.

Nami, M., & Bertels, K. (2007). A framework for autonomic computing systems. In *Proceedings of the IEEE International Conference on Self-Adaptive Systems* (pp. 85–90). IEEE.

NDSS Symposium. (2020). *Self-adaptive security systems and autonomic protection*. Internet Society.

RiskRecon, R. (2024). *The future of web application security: Addressing the rising risks.* RiskRecon White Paper.

TNO. (2022). Self-healing for cybersecurity: Architecture and implementation. TNO Publications.

TNO, M., et al. (2022). Self-healing for cybersecurity: Towards autonomous adaptive protection. *European Cybersecurity Review, 3*(1), 55–67

Villegas, N., Müller, H. A., Tamura, G., Duchien, L., & Casallas, R. (2011). A framework for evaluating quality-driven self-adaptive software systems. In *Proceedings of the 6th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* (pp. 80–89). ACM.

Zhao, H., & Li, C. (2024). Adaptive web application defense through reinforcement learning. *Computers & Security, 121,* 103–127.

Zhou, A., & Han, R. (2023). Adaptive intrusion response systems based on MAPE-K loop. *International Journal of Information Security Science, 12*(1), 58–70.