Browser Extension *Endpoint Security* Anti Spyware dan Data *Exfiltration* Berbasis *Rule based Java Script*

Bambang Purwanto[1)], Ricki Septian Nurpratama[2)], Robianto Herdana Sukirno[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: bambangrima78@gmail.com[1)], ricki.firewall@gmail.com[2)], robiantoherdana@gmail.com[3)]

Browser Extension Endpoint Security Anti Spyware and Data Exfiltration Berbasis Rule based Java Script

Abstract: *The expansion of web based applications has increased browser side security risks, particularly through malicious Java Script exploitation leading to data exfiltration. Conventional endpoint security mechanisms primarily emphasize network-layer monitoring, leaving client side browser activities less protected. This study proposes a browser extension-based endpoint security solution employing a rule based Java Script monitoring approach to detect spyware behavior and prevent unauthorized data transmission. Using the Research and Development (R&D) methodology, the system was designed, implemented and evaluated through controlled attack simulations. The extension monitors DOM access, local storage usage and outbound HTTP/HTTPS requests based on predefined detection rules. Experimental results across ten simulated scenarios demonstrate an 80% detection rate. The findings indicate that rule based client side monitoring offers a lightweight and practical approach to strengthening browser-level endpoint security.*

Keywords: Data Exfiltration, Endpoint Security, Browser Extension, Rule based Detection

Abstrak: *Peningkatan penggunaan aplikasi berbasis web memperbesar risiko keamanan pada sisi browser, khususnya lewat eksploitasi Java Script berbahaya yang dapat menyebabkan data exfiltration. Mekanisme endpoint security konvensional pada umumnya berfokus kepada pemantauan jaringan sehingga aktivitas pada sisi klien kurang terpantau secara optimal. Penelitian ini mengusulkan solusi endpoint security berbasis browser extension dengan pendekatan rule based untuk mendeteksi perilaku spyware dan mencegah transmisi data tanpa izin. Metode Research and Development (R&D) digunakan dalam proses perancangan, implementasi dan evaluasi sistem. Extension melakukan pemantauan terhadap akses DOM, penggunaan local storage serta permintaan HTTP/HTTPS keluar berdasarkan aturan deteksi yang telah ditentukan. Hasil pengujian pada sepuluh skenario simulasi menunjukkan tingkat deteksi sebesar 80%, sehingga pendekatan ini dinilai efektif dan ringan dalam meningkatkan keamanan endpoint pada browser.*

Kata kunci: Pencurian Data, Keamanan Endpoint, Ekstensi Browser, Deteksi Berbasis Aturan.

PENDAHULUAN

Perkembangan aplikasi berbasis *web* telah meningkatkan ketergantungan organisasi maupun individu terhadap layanan digital yang berjalan menggunakan *browser*. Namun, peningkatan kompleksitas aplikasi *web* modern juga diikuti dengan meningkatnya risiko kebocoran data dan serangan berbasis pada sisi klien. Cheng et al. (2021) menjelaskan bahwa pelanggaran data (*data breach*) pada organisasi sering kali dipicu oleh kelemahan di sistem aplikasi dan mekanisme perlindungan yang tidak memadai, sehingga menyebabkan eksposur informasi sensitif. Kondisi ini menunjukkan bahwa perlindungan terhadap data tidak hanya bergantung pada keamanan jaringan, tetapi juga pada mekanisme pengamanan di tingkat aplikasi dan pengguna akhir.

Salah satu vektor serangan yang semakin signifikan adalah serangan berbasis *browser* dan eksploitasi java script pada sisi klien. Hasan et al. (2022) menekankan bahwa *browser* modern memiliki permukaan serangan yang luas karena kemampuannya dalam mengeksekusi skrip dinamis dan mengakses berbagai komponen data, seperti *Document Object Model* (*DOM*), *cookie dan local storage*. Tian et al. (2021) juga menyatakan bahwa serangan *client side* pada aplikasi *web* modern semakin kompleks dan sering kali tidak terdeteksi oleh sistem keamanan konvensional yang berfokus pada *layer* jaringan.

Dalam konteks kebocoran data berbasis *web*, Sharma et al. (2023) mengungkapkan bahwa pola komunikasi keluar (*outbound traffic*) yang tidak terkontrol menjadi salah satu indikator utama terjadinya data *leakage*. Namun, mekanisme analitik keamanan yang digunakan untuk mendeteksi kebocoran data sering kali membutuhkan sumber daya komputasi yang cukup besar dan bergantung pada pendekatan berbasis pembelajaran mesin. Hal ini menimbulkan tantangan dalam implementasi sistem deteksi yang ringan dan dapat berjalan secara *real time* pada sisi klien.

Berbagai penelitian telah membandingkan pendekatan berbasis *machine learning* dan *rule based* dalam sistem deteksi keamanan. Sarker (2021) menyatakan bahwa meskipun *machine learning* memiliki kemampuan adaptif yang tinggi, pendekatan *rule based* lebih unggul dalam hal transparansi, efisiensi komputasi dan kemudahan audit. Temuan ini diperkuat oleh Rahimi dan Ghorbani (2023) yang menunjukkan bahwa model berbasis aturan tetap relevan dalam mendeteksi pola ancaman yang telah terdefinisi, khususnya pada lingkungan dengan kebutuhan respon cepat dan sumber daya terbatas.

Pendekatan *lightweight detection* juga menjadi perhatian dalam pengembangan sistem keamanan berbasis *web*. Ali et al. (2022) menekankan pentingnya sistem deteksi yang tidak membebani performa aplikasi, sementara Rahman dan Hasan (2025) mengusulkan model deteksi ringan berbasis aturan yang mampu mempertahankan efisiensi sistem tanpa mengorbankan efektivitas deteksi. Hal ini menunjukkan bahwa sistem keamanan yang efektif tidak hanya akurat, tetapi juga harus mempertimbangkan aspek performa dan stabilitas.

Meskipun berbagai penelitian telah mengkaji deteksi ancaman berbasis *web*, masih terdapat kebutuhan untuk mengimplementasikan mekanisme deteksi yang secara khusus bekerja pada sisi klien dengan pendekatan yang ringan dan terstruktur. Sebagian besar solusi yang ada

masih berorientasi pada sistem tingkat jaringan atau *server*, sehingga aktivitas mencurigakan yang terjadi langsung pada *browser* berpotensi tidak terpantau secara optimal.

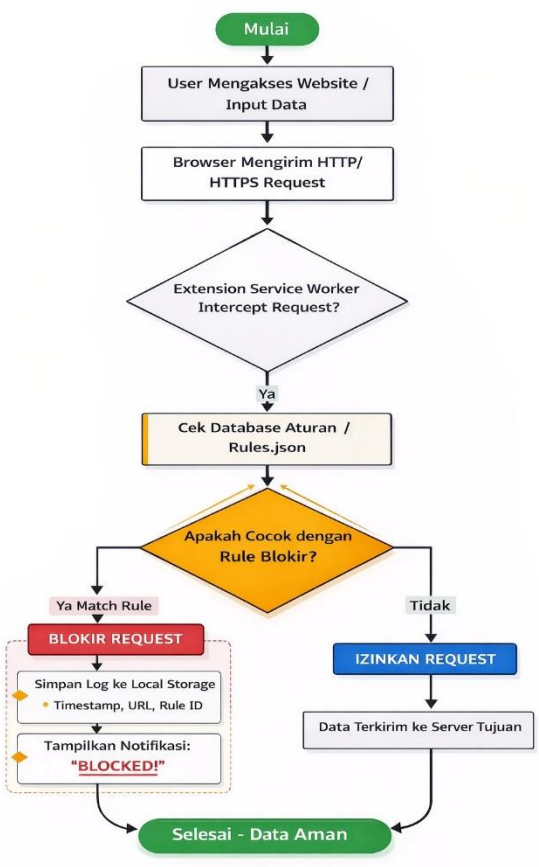
Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan mekanisme deteksi eksfiltrasi data berbasis *rule based* yang diimplementasikan pada lingkungan *browser* melalui pendekatan *client side monitoring*. Dengan memanfaatkan prinsip *lightweight detection* dan transparansi aturan, penelitian ini diharapkan dapat memberikan kontribusi terhadap penguatan keamanan *endpoint* pada sisi klien, khususnya dalam menghadapi ancaman kebocoran data berbasis *web*.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Research and Development* (*R&D*) untuk mengembangkan serta mengevaluasi sistem keamanan *endpoint* berbasis *browser* extension dalam mendeteksi aktivitas eksfiltrasi data pada sisi klien. Metode *R&D* dipilih karena memungkinkan proses pengembangan produk perangkat lunak dilakukan secara sistematis melalui tahapan perancangan, implementasi, validasi dan evaluasi kinerja (Sugiyono, 2022). Pendekatan ini relevan dalam penelitian yang berorientasi pada pengembangan teknologi yang dapat diuji efektivitasnya.

Tahap awal penelitian diawali dengan analisis kebutuhan sistem melalui studi literatur terhadap teknik data *exfiltration* berbasis *Java Script* serta mekanisme *client side monitoring*. Kajian ini bertujuan mengidentifikasi pola serangan yang umum terjadi pada lingkungan *browser*, termasuk akses terhadap *Document Object Model* (*DOM*), pengambilan token autentikasi dan transmisi data melalui permintaan *HTTP/HTTPS*. Hasil analisis ini digunakan sebagai dasar dalam merumuskan indikator perilaku mencurigakan yang akan diterjemahkan ke dalam aturan deteksi.

Tahap berikutnya adalah perancangan arsitektur sistem. Sistem dikembangkan dalam bentuk *browser* extension yang bekerja pada sisi klien dengan memanfaatkan content script untuk memantau interaksi terhadap elemen *DOM* serta API jaringan untuk menginspeksi komunikasi keluar. Arsitektur dirancang agar mampu melakukan pemantauan *real time* terhadap aktivitas skrip yang berjalan pada halaman *web* tanpa mengganggu pengalaman pengguna secara signifikan. Pendekatan ini sejalan dengan konsep *client side security monitoring* yang menekankan visibilitas langsung terhadap eksekusi aplikasi pada *browser*



Dengan alur kerja yang terstruktur sebagaimana ditunjukkan pada flowchart, sistem mampu melakukan proses deteksi secara sistematis dan *real time* pada sisi klien. Mekanisme pencocokan berbasis aturan memungkinkan identifikasi aktivitas mencurigakan dilakukan secara cepat tanpa membebani performa *browser* secara signifikan. Oleh karena itu, desain arsitektur dan alur proses ini menjadi fondasi utama dalam mendukung efektivitas sistem dalam mencegah eksfiltrasi data melalui komunikasi *HTTP/HTTPS* yang tidak sah.

Implementasi sistem dilakukan menggunakan bahasa pemrograman *Java Script* dengan memanfaatkan arsitektur ekstensi *browser* modern. Modul utama sistem terdiri dari komponen *monitoring DOM*, pengawas permintaan *HTTP/HTTPS* serta rule engine yang berfungsi mengevaluasi aktivitas berdasarkan aturan yang telah ditentukan. Aturan deteksi disusun dalam format terstruktur sehingga dapat diperbarui secara berkala sesuai perkembangan pola serangan. Pendekatan *rule based* dipilih karena menawarkan transparansi logika deteksi serta efisiensi komputasi yang lebih baik dibandingkan pendekatan berbasis *machine learning* dalam konteks *monitoring real time* (Sarker, 2021).

Setelah tahap implementasi, sistem diuji melalui simulasi sepuluh skenario serangan data *exfiltration* berbasis *Java Script*. Setiap skenario dirancang untuk merepresentasikan teknik yang umum digunakan, seperti pengiriman data form tanpa otorisasi, ekstraksi data dari local storage serta pengiriman parameter terenkripsi ke *DOM*ain eksternal. Evaluasi dilakukan dengan mengukur tingkat deteksi berdasarkan jumlah skenario yang berhasil diidentifikasi oleh sistem dibandingkan dengan total skenario pengujian. Pendekatan evaluasi ini mengikuti metodologi pengujian sistem deteksi keamanan yang digunakan dalam penelitian sebelumnya. Rumus tingkat deteksi yang digunakan adalah:

$$Detection\ Rate = \frac{Jumlah\ Deteksi\ Berhasil}{Total\ Skenario} \times 100\%$$

Tingkat deteksi dihitung menggunakan perbandingan antara jumlah deteksi yang benar dengan total skenario uji, kemudian dinyatakan dalam bentuk persentase. Selain itu, evaluasi juga mempertimbangkan stabilitas sistem dan dampaknya terhadap performa *browser* selama proses *monitoring* berlangsung. Dengan tahapan tersebut, metode penelitian ini tidak hanya berfokus pada pengembangan sistem, tetapi juga pada pengujian efektivitasnya secara terukur dalam lingkungan simulasi yang terkontrol.

HASIL PENELITIAN

1. Hasil penelitian ini diperoleh melalui proses implementasi dan pengujian sistem *browser* extension *endpoint security* berbasis *rule based Java Script* yang telah dirancang pada tahap sebelumnya. Pengujian dilakukan untuk mengevaluasi kemampuan sistem dalam mendeteksi aktivitas eksfiltrasi data pada sisi klien melalui simulasi skenario serangan yang terkontrol.

Sebanyak sepuluh skenario serangan dirancang untuk merepresentasikan teknik eksfiltrasi data yang umum digunakan pada aplikasi berbasis *web*. Skenario tersebut mencakup pengiriman data form tanpa persetujuan pengguna, pengambilan token autentikasi dari localStorage, manipulasi parameter URL serta transmisi data ke *DOM*ain eksternal yang tidak termasuk dalam daftar *DOM*ain terpercaya. Perancangan skenario ini mengacu pada karakteristik

teknik data *exfiltration* yang dijelaskan dalam penelitian sebelumnya.

Selama proses pengujian, sistem melakukan pemantauan terhadap aktivitas *DOM*, penggunaan API penyimpanan lokal serta permintaan *HTTP/HTTPS* yang dikirimkan dari *browser* ke *server* eksternal. Setiap aktivitas yang terdeteksi kemudian dievaluasi oleh rule engine untuk menentukan apakah pola tersebut memenuhi kriteria eksfiltrasi data yang telah didefinisikan pada tahap perancangan.

Hasil pengujian menunjukkan bahwa dari sepuluh skenario serangan yang disimulasikan, sistem berhasil mendeteksi delapan skenario secara tepat, sementara dua skenario tidak terdeteksi karena pola aktivitasnya tidak sepenuhnya memenuhi aturan yang telah ditentukan. Dengan demikian, tingkat deteksi sistem dapat dihitung sebagai berikut:

$$Detection\ Rate = \frac{8}{10} \times 100\% = 80\%$$

Tingkat deteksi sebesar 80% menunjukkan bahwa pendekatan *rule based* yang diterapkan mampu mengidentifikasi mayoritas pola eksfiltrasi data yang bersifat eksplisit. Hasil ini konsisten dengan temuan yang menyatakan bahwa sistem berbasis aturan efektif dalam mendeteksi pola serangan yang telah terdefinisi sebelumnya.

Selain tingkat deteksi, evaluasi juga dilakukan terhadap stabilitas dan performa sistem selama proses *monitoring* berlangsung. Berdasarkan observasi, ekstensi tidak menimbulkan penurunan performa *browser* yang signifikan dan tidak mengganggu pengalaman pengguna dalam mengakses halaman *web*. Hal ini menunjukkan bahwa pendekatan *rule based* relatif ringan dibandingkan metode berbasis *machine learning* yang membutuhkan proses komputasi tambahan (Sarker, 2021).

Namun demikian, dua skenario yang tidak terdeteksi menunjukkan bahwa sistem masih memiliki keterbatasan dalam mengenali variasi pola eksfiltrasi yang dimodifikasi atau disamarkan. Hal ini menegaskan pentingnya pembaruan aturan deteksi secara berkala untuk meningkatkan cakupan deteksi terhadap teknik serangan yang terus berkembang.

Secara keseluruhan, hasil penelitian menunjukkan bahwa sistem *browser* extension *endpoint security* yang dikembangkan mampu berfungsi sesuai dengan tujuan penelitian, yaitu mendeteksi aktivitas eksfiltrasi data pada sisi klien dengan tingkat efektivitas yang terukur.

Tabel 1 merangkum secara komprehensif hasil dari berbagai sumber dan referensi terpilih yang telah dianalisis dan diekstraksi secara sistematis. Pendekatan ini digunakan untuk memastikan kualitas, transparansi dan relevansi data untuk mendukung pencapaian penelitian. Tabel ini mencerminkan proses tinjauan literatur yang terstruktur dan sistematis serta menjadi landasan yang kuat dalam penyajian temuan dan pembangunan argumentasi ilmiah pada penelitian yang sedang dikembangkan.

No	Referensi & Penulis	Fokus Penelitian	Temuan Utama	Relevansi terhadap Penelitian
1	Rahman & Hasan (2025)	Model deteksi ringan berbasis aturan untuk ancaman *web*	Pendekatan *rule based* ringan efektif tanpa beban komputasi tinggi	Mendukung pemilihan metode *rule based* pada ekstensi *browser*

2	Sarker (2021)	Perbandingan *machine learning* dan *rule based* dalam keamanan siber	*Rule based* lebih transparan dan efisien untuk deteksi *real time*	Menguatkan alasan penggunaan rule engine pada sisi klien
3	Cheng et al. (2021)	Analisis kebocoran data perusahaan	Eksfiltrasi data menjadi penyebab utama pelanggaran keamanan	Menjadi dasar urgensi deteksi data *exfiltration*
4	Hasan et al. (2022)	Tinjauan mekanisme keamanan *browser* dan mitigasi serangan *client side*	*Browser* rentan terhadap manipulasi *Java Script* dan *DOM*	Mendukung kebutuhan *monitoring* pada sisi klien
5	Sharma et al. (2023)	Analitik keamanan untuk deteksi kebocoran data berbasis *web*	Analisis pola komunikasi keluar meningkatkan akurasi deteksi	Relevan dengan *monitoring HTTP/HTTPS* pada ekstensi
6	Ali et al. (2022)	Sistem deteksi ringan untuk serangan *web*	Model ringan mempertahankan performa sistem	Selaras dengan kebutuhan ekstensi yang tidak membebani *browser*
7	Tian et al. (2021)	Deteksi serangan *client side* pada aplikasi *web* modern	*Client side monitoring* meningkatkan visibilitas ancaman	Mendukung pendekatan *monitoring DOM* dan skrip
8	Rahimi & Ghorbani (2023)	Perbandingan *rule based* dan learning-based pada ancaman *web*	*Rule based* efektif untuk pola serangan yang telah diketahui	Menguatkan desain sistem berbasis aturan

Tabel 1. Ringkasan temuan utama dari berbagai referensi terkait deteksi eksfiltrasi data dan keamanan sisi klien pada *browser* menggunakan pendekatan *rule based* serta mekanisme *monitoring* berbasis ekstensi *browser*.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa sistem *browser* extension *endpoint security* berbasis *rule based Java Script* mampu mencapai tingkat deteksi sebesar 80% dalam sepuluh skenario simulasi eksfiltrasi data. Capaian ini menunjukkan bahwa pendekatan *rule based* efektif dalam mengidentifikasi pola serangan yang telah terdefinisi sebelumnya. Temuan ini sejalan dengan penelitian yang menyatakan bahwa sistem berbasis aturan memiliki tingkat akurasi yang baik untuk mendeteksi pola serangan yang bersifat eksplisit dan terstruktur.

Efektivitas sistem dalam mendeteksi delapan dari sepuluh skenario menunjukkan bahwa *monitoring* pada sisi klien memberikan visibilitas tambahan yang tidak selalu tersedia pada mekanisme keamanan berbasis jaringan. menekankan bahwa aktivitas komunikasi keluar dari *browser* sering kali tidak dianalisis secara mendalam oleh sistem keamanan konvensional. Dengan memanfaatkan *browser* extension sebagai lapisan *monitoring* tambahan, penelitian ini menunjukkan bahwa deteksi dapat dilakukan langsung pada titik eksekusi skrip, sehingga

meningkatkan peluang identifikasi aktivitas mencurigakan.

Dari sisi performa, pendekatan *rule based* yang diterapkan dalam penelitian ini terbukti tidak memberikan dampak signifikan terhadap kinerja *browser*. Hal ini mendukung argumentasi Sarker (2021) yang menyatakan bahwa metode berbasis aturan lebih ringan secara komputasi dibandingkan model *machine learning*, terutama dalam konteks pemantauan *real time* dengan sumber daya terbatas. Transparansi aturan juga menjadi keunggulan karena memungkinkan proses audit dan pembaruan dilakukan dengan lebih mudah.

Namun demikian, dua skenario yang tidak terdeteksi mengindikasikan adanya keterbatasan dalam cakupan aturan deteksi. Serangan yang dimodifikasi atau menggunakan teknik obfuscation berpotensi tidak teridentifikasi apabila tidak sesuai dengan pola yang telah ditentukan. Kondisi ini sesuai dengan temuan yang menyebutkan bahwa sistem deteksi berbasis pola memiliki keterbatasan terhadap variasi teknik serangan yang terus berkembang.

Selain itu, penelitian menunjukkan bahwa kompleksitas aplikasi *web* modern menyebabkan variasi interaksi *DOM* yang semakin dinamis. Hal ini menuntut mekanisme deteksi yang adaptif dan mampu memperbarui aturan secara berkala. Oleh karena itu, meskipun pendekatan *rule based* terbukti efektif dan ringan, pengembangan lanjutan dapat mempertimbangkan integrasi metode *hybrid* untuk meningkatkan ketahanan terhadap serangan *zero day*.

Secara keseluruhan, pembahasan ini menunjukkan bahwa sistem yang dikembangkan telah memenuhi tujuan penelitian dalam menyediakan mekanisme *client side monitoring* untuk mendeteksi eksfiltrasi data. Kontribusi utama penelitian ini terletak pada implementasi *rule based detection* secara langsung pada lingkungan *browser* melalui ekstensi, yang memberikan alternatif solusi *endpoint security* yang ringan, transparan dan mudah diimplementasikan.

PENUTUP

Penelitian ini berhasil mengembangkan sistem *browser* extension *endpoint security* berbasis *rule based Java Script* yang dirancang untuk mendeteksi aktivitas eksfiltrasi data pada sisi klien. Melalui pendekatan *Research and Development* (*R&D*), sistem dirancang, diimplementasikan dan diuji dalam lingkungan simulasi terkontrol yang merepresentasikan sepuluh skenario serangan berbasis *Java Script*. Hasil pengujian menunjukkan tingkat deteksi sebesar 80% yang mengindikasikan bahwa pendekatan *rule based* efektif dalam mengidentifikasi pola eksfiltrasi data yang telah terdefinisi. Sistem mampu memonitor akses *DOM*, penggunaan local storage serta komunikasi *HTTP/HTTPS* secara *real time* tanpa menimbulkan penurunan performa *browser* yang signifikan. Temuan ini memperkuat argumentasi bahwa mekanisme *client side monitoring* dapat menjadi lapisan perlindungan tambahan terhadap ancaman berbasis skrip pada lingkungan *browser*. Kontribusi utama penelitian ini terletak pada implementasi model deteksi berbasis aturan yang ringan, transparan dan mudah diperbarui. Pendekatan ini memberikan alternatif solusi *endpoint security* yang praktis, khususnya pada konteks perlindungan sisi klien yang belum sepenuhnya terakomodasi oleh sistem keamanan berbasis jaringan.

DAFTAR PUSTAKA

Rahman, M., & Hasan, R. (2025). Lightweight *rule based detection* model for *web* threats. Future Internet, 17(1), 15. https://doi.org/10.3390/fi17010015

Sarker, I. H. (2021). *Machine learning* versus *rule based* systems in cyber*security*: A comparative analysis. Journal of Network and Computer Applications, 178, 102915. https://doi.org/10.1016/j.jnca.2020.102915

Cheng, L., Liu, F., & Yao, D. (2021). Enterprise *data breach*: Causes, challenges, prevention and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 11(5), e1391. https://doi.org/10.1002/widm.1391

Hasan, M., Islam, M. M., & Rahman, M. (2022). A review of *browser security* mechanisms and *client side* attack mitigation techniques. Electronics, 11(18), 2895. https://doi.org/10.3390/electronics11182895

Sharma, S., Chen, Y., & Sheth, A. (2023). *Security* analytics for detecting *web*-based data *leakage* attacks. Future Generation Computer Systems, 140, 52–64. https://doi.org/10.1016/j.future.2022.11.021

Ali, S., Murad, M., & Khan, A. (2022). A lightweight intrusion *detection* approach for *web*-based attacks. Applied Sciences, 12(4), 1987. https://doi.org/10.3390/app12041987

Tian, R., Batten, L., & Versteeg, S. (2021). *Client side* attack *detection* in modern *web* applications. Computers & *Security*, 105, 102246. https://doi.org/10.1016/j.cose.2021.102246

Rahimi, S., & Ghorbani, A. (2023). *Rule based* versus learning-based *detection* models for *web security* threats. Journal of Cyber*security*, 9(1), tyad012. https://doi.org/10.1093/cybsec/tyad012