Avaliação de Cobertura de SAST e LLM em Plataformas de Blockchain Permissionada para Supply Chain Automotiva com base no OWASP

Glauco Scheffel[1], Luiz Camargo[1], Gilson Sohn Junior[1], Pedro de Souza[1], Charles Miers[1], Marcos A. Simplicio Junior[2], Maurício Pillon[1,2]

[1] Universidade do Estado de Santa Catarina (UDESC) – Joinville – SC – Brasil
[2] Escola Politécnica, Universidade de São Paulo (USP) – São Paulo – SP – Brasil

{glauco.scheffel,charles.miers,mauricio.pillon}@udesc.br
{lc.camargo,gilson.sj,phsd.souza}@edu.udesc.br
{mjunior,mpillon}@larc.usp.br

Abstract. *Permissioned blockchain (BC) platforms applied to the supply chain expand the attack surface by combining smart contracts, APIs, identities, and off-chain components, requiring security analysis approaches that go beyond conventional standards. This work investigates the extent to which traditional SAST tools cover the risks of these platforms and what gaps emerge when faced with LLM-assisted contextual analysis, using the OWASP Top 10:2025 as a reference. The assessment was conducted on two industrial platforms based on Hyperledger Fabric, HERMES and MoVChain, combining SonarCloud, Semgrep, and LLM-assisted analysis. We identified 124 findings in first-party code and artifacts, organized into 25 consolidated risk categories, with low overlap between sources (only 12%). The results show that combining these approaches, and human validation, strengthens coverage in secure development processes for industrial environments with permissioned blockchains.*

Resumo. *As plataformas de blockchain (BC) permissionadas aplicadas à cadeia de suprimentos ampliam a superfície de ataque ao combinarem contratos inteligentes, APIs, identidades e componentes off-chain, o que exige abordagens de análise de segurança que vão além dos padrões convencionais. Este trabalho investiga em que medida ferramentas tradicionais de SAST cobrem os riscos dessas plataformas e quais lacunas emergem diante de uma análise contextual assistida por LLM, tendo como referência o OWASP Top 10:2025. A avaliação foi conduzida em duas plataformas industriais baseadas em Hyperledger Fabric HERMES e MoVChain, combinando SonarCloud, Semgrep e análise assistida por LLM. Foram identificados 124 achados em código próprio, organizados em 25 categorias consolidadas de risco, com baixa sobreposição entre as fontes (apenas 12%). Os resultados evidenciam que a combinação dessas abordagens, com validação humana, fortalece a cobertura em processos de desenvolvimento seguros para ambientes industriais com blockchains permissionadas.*

1. Introdução

A cadeia de suprimentos automotiva envolve múltiplas organizações, jurisdições e requisitos regulatórios associados à origem, qualidade e sustentabilidade dos produtos [Nowak 2025]. Nesse contexto, plataformas de blockchain (BC) permissionadas são

usadas para prover auditabilidade, integridade e compartilhamento controlado de dados. Contudo, ao combinarem aplicações *Web*, API, contratos inteligentes, identidades e integrações *off-chain*, ampliam a superfície de ataque [Liang et al. 2024]. Este trabalho analisa duas plataformas de BC permissionadas aplicadas à indústria automotiva do Mercosul: HERMES [Hopfer et al. 2026] e MoVChain [Souza et al. 2026]. Ambas foram concebidas para demandas reais de BECOMEX, organização certificada pela ISO/IEC 27001 [International Organization for Standardization 2022], e avaliadas aqui apenas de forma agregada, por se tratar de política interna.

Essas plataformas introduzem riscos além das vulnerabilidades convencionais de aplicações *Web*, envolvendo configurações de canais e coleções privadas, políticas de endosso, identidades, credenciais, componentes *off-chain* e contratos inteligentes. O problema investigado concentra-se na adequação e nas lacunas de cobertura das abordagens de análise avaliadas, utilizando o *Open Worldwide Application Security Project* (OWASP) Top 10:2025 como referência para categorização dos achados. Assim, este trabalho é guiado pela questão de pesquisa: *em que medida ferramentas tradicionais de Teste Estático de Segurança de Aplicativos (SAST), já incorporadas a processos corporativos de desenvolvimento seguro, identificam riscos de segurança em plataformas de BC permissionadas, e quais lacunas de cobertura emergem quando comparadas a uma análise contextual assistida por Large Language Model (LLM)?* Para respondê-la, apresenta-se uma avaliação comparativa das duas plataformas, combinando SonarCloud [SonarSource 2026], Semgrep [Semgrep 2026] e análise contextual assistida por LLM, com categorização pelo OWASP Top 10:2025 [OWASP Foundation 2025].

Este trabalho apresenta uma avaliação comparativa de segurança em plataformas de BC permissionadas desenvolvidas em cooperação universidade–indústria. As principais contribuições são: (i) a avaliação da adequação de ferramentas tradicionais de SAST em plataformas de BC permissionadas, comparando SonarCloud, Semgrep e uma execução de análise contextual assistida por LLM quanto à cobertura observada[1], complementaridade e limitações, com categorização pelo OWASP Top 10:2025; (ii) a consolidação de 25 categorias de risco, distinguindo achados comuns, parcialmente sobrepostos e exclusivos de cada abordagem; e (iii) a discussão sobre o uso de análise assistida por LLM em processos de desenvolvimento seguro com BC permissionada.

O restante do artigo está organizado como segue. A Seção 2 apresenta a fundamentação teórica; a Seção 2.1, os trabalhos relacionados; e a Seção 3, o estudo de caso e o escopo da avaliação e os resultados.

2. Fundamentação Teórica

As plataformas HERMES e MoVChain são utilizadas neste trabalho como referências de domínio para problemas de rastreabilidade na cadeia automotiva. Nesse contexto, requisitos associados à origem preferencial, ao cálculo de *Regional Value Content* (RVC), à emissão ou validação de Certificados de Origem (COs) e a indicadores *Environmental, Social, and Governance* (ESG) demandam mecanismos capazes de prover rastreabilidade, auditabilidade e proteção de dados sensíveis entre múltiplas organizações. Tais requisitos

[1]Cobertura observada refere-se ao conjunto de achados e categorias identificados por cada fonte no *snapshot* analisado, e não a uma taxa absoluta de detecção sobre um universo completo de vulnerabilidades conhecidas.

motivam o uso de plataformas digitais que registrem evidências verificáveis, controlem o acesso a dados estratégicos e apoiem processos de auditoria sem expor integralmente informações comerciais ou produtivas dos participantes.

Em plataformas de BC permissionadas, como *Hyperledger Fabric* (HLF), a operação depende de contratos inteligentes (*chaincodes*), canais, coleções privadas, políticas de endosso e identidades, que restringem o acesso e controlam a validação de transações no *ledger*, mas também ampliam a superfície de ataque diante de configurações inadequadas ou falhas nesses mecanismos. Assim, a avaliação de segurança deve considerar código-fonte, infraestrutura, configurações e relações arquiteturais entre os artefatos da plataforma.

A análise estática de segurança de aplicações, ou SAST, inspeciona código-fonte ou bytecode sem executar a aplicação, permitindo identificar padrões de fraqueza, vulnerabilidades e violações de boas práticas ainda durante o desenvolvimento [Deshapriya et al. 2026, Oka 2021]. Neste trabalho, SonarCloud e Semgrep são ferramentas tradicionais de SAST, cujos achados são categorizados com base no OWASP Top 10:2025. A Teste Dinâmico de Segurança de Aplicações (DAST) não é o foco deste estudo, que se concentra na análise estática e na análise contextual assistida por LLM.

A análise assistida por LLM foi empregada como abordagem complementar com Claude Opus 4.7 com a licença da BECOMEX, e não como substituta das ferramentas de SAST. Seu uso busca apoiar a identificação de riscos que dependem da correlação entre código, configurações, contratos inteligentes e componentes distribuídos em múltiplos arquivos. Como LLMs podem produzir falsos positivos, falsos negativos e respostas variáveis [Ameen et al. 2026, Halder et al. 2026], seus resultados foram tratados como evidências auxiliares, sujeitas à validação humana detalhada na Seção 3.1.

2.1. Trabalhos Relacionados

O contexto da busca bibliográfica apoiou-se no método PICOC [Nishikawa-Pacher 2022], aplicado a Cadeia de Suprimentos Automotiva (CSA), indústria, OWASP, BC e abordagens correlatas. A CSA é foco dos trabalhos [Liao et al. 2026, Alsadi et al. 2023, Aideyan et al. 2025], todos publicados nos últimos três anos, sendo dois destes associados ao contexto industrial, segundo critério de interesse deste estudo (Tabela 1). Entretanto, não há menção ao uso de OWASP nesses trabalhos. O único estudo com preocupação explícita em avaliação de segurança é [Liao et al. 2026], baseado em IDS/GX (*Industrial Data Space* e GAIA-X). De acordo com esses critérios, o trabalho com maior aderência às características das plataformas analisadas é [Alsadi et al. 2023]. Todavia, o estudo não considera avaliação de segurança baseada no OWASP nem análise por SAST. Assim, a avaliação de segurança em aplicações BC voltadas à CSA industrial permanece um tema relevante e pouco explorado pela comunidade científica.

Tabela 1. Comparação dos trabalhos relacionados.

Critério	[Liao et al. 2026]	[López et al. 2025]	[Fasha et al. 2024]	[Alsadi et al. 2023]	[Aideyan et al. 2025]	[Budiyanto et al. 2024]	Proposta
CSA	✓	-	-	✓	✓	-	✓
Indústria	✓	-	-	✓	-	-	✓
OWASP	-	✓	✓	-	-	✓	✓
Blockchain	-	-	-	✓	✓	-	✓
Outras	IDS/GX	-	-	-	-	-	-

3. Estudo de Caso e Escopo da Avaliação

Este trabalho apresenta uma avaliação de segurança utilizando o OWASP Top 10:2025 como taxonomia de referência, aplicada a duas plataformas de BC permissionadas no contexto de CSA industrial. O estudo analisa os resultados obtidos com três abordagens de avaliação de segurança: SonarCloud, Semgrep e análise assistida por LLM, aplicadas às plataformas desenvolvidas em um contexto universidade–indústria: HERMES, voltada à rastreabilidade de origem e ao cálculo de RVC [Hopfer et al. 2026], e MoVChain, direcionada à rastreabilidade de indicadores ESG [Souza et al. 2026]. Ambas são utilizadas como estudos de caso industriais por combinarem auditabilidade, compartilhamento controlado de dados e preservação de informações estratégicas entre organizações da CSA.

O escopo inclui os artefatos necessários à operação das plataformas em ambientes de desenvolvimento e homologação: código-fonte próprio, APIs, contratos inteligentes, *scripts* de infraestrutura, arquivos de orquestração, componentes *off-chain* e configurações de BC permissionada. Os códigos de terceiros não modificados foram separados da análise principal, de modo que os resultados refletissem prioritariamente riscos introduzidos ou configurados no contexto das plataformas avaliadas. As plataformas adotam mecanismos como *Role-Based Access Control* (RBAC), coleções privadas, canais isolados, *hashes* SHA-256 em *ledger*, contratos inteligentes, assinaturas digitais, SmartBFT e endosso multi-organização, que garantem controle de acesso, integridade e auditoria posterior.

A avaliação foi conduzida como um estudo comparativo de segurança estática sobre o mesmo *snapshot* dos repositórios MoVChain e HERMES, abrangendo código-fonte, *scripts* de infraestrutura, arquivos de orquestração e componentes de apoio. Foram utilizadas três fontes de análise: (i) SonarCloud, com regras *Security* e *Maintainability*; (ii) Semgrep Code, com regras *Security*; e (iii) análise contextual com Claude Opus 4.7 [Anthropic 2026], instrumentada pela Claude OWASP Skill [Agam 2026][2]. A análise via LLM foi conduzida em sessão única por plataforma, com a Claude OWASP Skill carregada e o repositório completo (código, *chaincodes*, Dockerfiles e manifestos de infraestrutura) fornecido ao modelo, gerando saída padronizada por achado (escopo, severidade sugerida, evidência, recomendação), sem refinamento iterativo do *prompt* nem ajuste de hiperparâmetros além do padrão do ambiente. A análise considerou apenas artefatos próprios das plataformas, após a remoção de duplicidades, a segregação do código de terceiros não modificado e exclusão de comportamentos esperados em homologação. Um *achado próprio* é um problema identificado em código programado pelos autores no desenvolvimento da HERMES ou da MoVChain, e não em bibliotecas ou componentes de terceiros não modificados. As severidades nativas de SonarCloud e Semgrep, e a severidade sugerida pela LLM e revisada pelos autores, foram harmonizadas em duas faixas – alta criticidade e média/baixa –, e os achados foram mapeados manualmente para o OWASP Top 10:2025 [OWASP Foundation 2025], com apoio da *Common Weakness Enumeration* (CWE) quando disponível; decisões fronteiriças foram registradas no mesmo repositório [Scheffel et al. 2026].

[2]Versão: commit `f1e5059` (28/abr/2026, "Add OWASP Top 10 for LLM Applications (2025) coverage"). Cópia congelada da *skill* e instruções preservada em repositório de acesso restrito, disponível mediante solicitação aos autores [Scheffel et al. 2026].

3.1. Resultados da Comparação

Após a segregação do código de terceiros, SonarCloud, Semgrep e análise via LLM produziram volumes próximos de achados próprios, indicando que nenhuma das abordagens dominou isoladamente a identificação de ocorrências. Apesar dessa proximidade quantitativa, os resultados diferiram em perfil: as ferramentas SAST concentraram-se em achados de média/baixa criticidade, enquanto a análise via LLM distribuiu-se de forma mais heterogênea, incluindo achados críticos e altos. Entre as plataformas avaliadas, a distribuição foi mais equilibrada no Semgrep e na análise via LLM, ao passo que o SonarCloud concentrou mais ocorrências na HERMES.

Os achados próprios foram mapeados manualmente para o OWASP Top 10:2025, com base na CWE ou na mensagem da regra. Dois achados do SonarCloud sem correspondência direta foram excluídos do mapeamento; a Figura 1(a) considera apenas achados classificados nas categorias OWASP. Essa síntese evidencia diferenças relevantes entre as ferramentas: o SonarCloud apresenta maior concentração em falhas criptográficas, o Semgrep destaca problemas de configuração, e a análise via LLM distribui seus achados por um conjunto mais amplo de categorias. A Figura 1(b) confirma essa leitura: a interseção entre as fontes foi limitada, sugerindo complementaridade – a maior parte das categorias foi identificada por apenas uma fonte, com destaque para as exclusivas da análise via LLM.

(a) Achados por categoria OWASP Top 10:2025.

Cat.	Tema	Sonar	Semgrep	Claude
A01	Acesso	0	5	6
A02	Configuração	14	31	12
A03	Suprimentos	1	0	4
A04	Criptografia	28	2	5
A05	Injeção	2	1	2
A06	Design	1	0	2
A07	Autenticação	0	0	2
A08	Falhas de integridade	0	0	0
A09	Registro/Alerta	0	0	4
A10	Falhas ao lidar com condições de exceção	0	0	0
Total		**46**	**39**	**37**

(b) Interseção entre fontes detectoras.

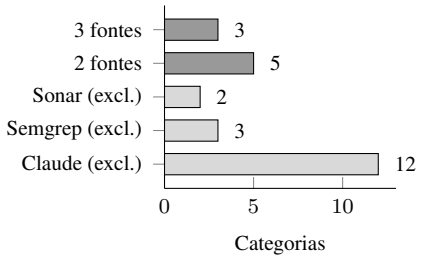

Figura 1. Síntese dos achados próprios por categoria OWASP Top 10:2025: (a) contagem por fonte; e (b) das 25 categorias consolidadas, 12 foram exclusivas da análise via LLM, 3 do Semgrep e 2 do SonarCloud, contra apenas 3 (12%) identificadas simultaneamente pelas três fontes.

O SonarCloud mostrou maior aderência a padrões sintáticos, fluxos de dados e *sinks* conhecidos, com destaque para A04, Falhas Criptográficas, principalmente pela detecção textual de segredos. Também identificou achados de alta criticidade, como *path traversal* e reflexão de entrada controlada pelo usuário na MoVChain, reforçando sua utilidade para vulnerabilidades reconhecíveis por regras estáticas. O Semgrep apresentou perfil complementar, com maior sensibilidade a problemas de configuração e infraestrutura. Seus achados concentraram-se em A02, Configuração Incorreta de Segurança, especialmente em manifestos Kubernetes e Dockerfiles. Isso reforça seu papel na identificação de fragilidades de implantação e configuração, complementando o SonarCloud em código e práticas criptográficas. A análise via LLM ampliou a cobertura para riscos dependentes de contexto arquitetural, especialmente no ambiente HLF. Entre os exemplos identificados estão *Transport Layer Security* (TLS) desabilitado no *chaincode Chaincode as a Service* (CCaaS), política de endosso permissiva, coleções privadas com permissões de

escrita abertas e condições de corrida em operações de atualização. Esses achados indicam que a análise contextual pode revelar problemas menos evidentes para ferramentas SAST tradicionais, embora seus resultados devam ser tratados como evidências auxiliares e submetidos à validação humana. Essa validação consistiu na inspeção manual de cada achado (arquivo, configuração ou trecho indicado) por dois autores do desenvolvimento das plataformas, seguida de discussão conjunta; nenhum achado foi descartado nesta execução, o que reflete apenas o conjunto analisado, sem implicar ausência geral de falsos positivos em outras execuções.

Em conjunto, os resultados sugerem complementaridade, e não substituição, entre SonarCloud, Semgrep e análise via LLM: os SASTs oferecem maior reprodutibilidade para padrões conhecidos de código e configuração, enquanto o LLM explora relações entre artefatos e decisões arquiteturais específicas de blockchain permissionada.

4. Considerações Finais

Este trabalho avaliou a segurança das plataformas MoVChain e HERMES por meio de SonarCloud, Semgrep e análise contextual assistida por LLM, com categorização pelo OWASP Top 10:2025. As três abordagens identificaram 124 achados em código próprio, organizados em 25 categorias consolidadas. Apenas três das 25 categorias consolidadas (12,0%) apareceram simultaneamente nas três fontes, evidenciando baixa interseção entre os resultados. Os achados indicam que SonarCloud e Semgrep oferecem cobertura mais reprodutível para padrões conhecidos de código, segredos/chaves e configurações, enquanto a análise via LLM, na execução considerada, evidenciou riscos arquiteturais específicos de HLF que não foram identificados pelas configurações e regras das ferramentas SAST utilizadas neste estudo. Portanto, os resultados não sustentam a substituição de ferramentas SAST por LLMs; ao contrário, indicam que sua combinação, com validação humana, pode ampliar a cobertura em avaliações de segurança de plataformas de BC permissionadas.

Como limitações, o estudo considerou duas plataformas em desenvolvimento/homologação, um conjunto específico de ferramentas e uma única execução por plataforma da análise assistida por LLM, sem controle dos autores sobre hiperparâmetros. Como trabalhos futuros, pretende-se repetir a análise via LLM em múltiplas execuções e modelos, alinhado a estudos como o SecLens [Halder et al. 2026], comparar sistematicamente com ferramentas especializadas, incluir análises dinâmicas, investigar a cobertura de ferramentas para HLF – dada a escassez de soluções públicas para detecção de vulnerabilidades em *chaincodes* [Li et al. 2022] – e formalizar o procedimento como fluxo reutilizável para outras plataformas de BC permissionada.

Agradecimentos

Este trabalho foi desenvolvido no âmbito do Programa de Pós-Graduação em Computação Aplicada (PPGCAP), em parceria com BECOMEX, LARC/USP e LabP2D/UDESC. Os autores agradecem o apoio da CAPES (Código de Financiamento 001), FAPESC, FAPESP, do CNPq (Processo nº 307732/2023-1), da Ripple University Blockchain Research Initiative e da BECOMEX.

Referências

Agam, M. (2026). OWASP Security Skill for Claude Code. https://github.com/agamm/claude-code-owasp. Acesso em: 17 maio 2026.

Aideyan, I., Pesé, M., and Brooks, R. (2025). Advancing automotive software supply chain security: A blockchain-reproducible build approach. In *2025 NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium*, Novi, Michigan, United States.

Alsadi, M., Arshad, J., Ali, J., Prince, A., and Shishank, S. (2023). Trucert: Blockchain-based trustworthy product certification within autonomous automotive supply chains. *Computers and Electrical Engineering*, 109:108738.

Ameen, M. R., Alam, M. T. U., and Islam, A. (2026). QASecClaw: A multi-agent llm approach for false positive reduction in static application security testing.

Anthropic (2026). Introducing Claude Opus 4.7. https://www.anthropic.com/news/claude-opus-4-7. Acesso em: 17 maio 2026.

Budiyanto, S., Silalahi, L. M., Hakim, A. R., Hamid, A., and Hanafi, D. (2024). Vulnerability analysis on internet of things (iot) networks using raspberry pi and open web application security project (owasp). In *2024 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE)*, pages 58–63.

Deshapriya, L., Licorish, S. A., and Woodford, B. J. (2026). Understanding warnings generated by pmd and sonarqube, their rules and compliance to established coding standards. *Science of Computer Programming*, 252.

Fasha, M., Rub, F. A., Matar, N., Sowan, B., Al Khaldy, M., and Barham, H. (2024). Mitigating the owasp top 10 for large language models applications using intelligent agents. In *2024 2nd International Conference on Cyber Resilience (ICCR)*, pages 1–9.

Halder, S., Saxena, S., Shrish, K. K., and M, T. (2026). SecLens: Role-specific evaluation of llms for security vulnerability detection.

Hopfer, K. B., Junior, G. S., Camargo, L. C., and Pillon, M. A. (2026). HERMES: Impacto de algoritmos de congestionamento no processo de certificação de origem. In *Anais do ERAD/RS 2026 – Fórum de Iniciação Científica e Pós-Graduação*, Bagé, RS, Brasil.

International Organization for Standardization (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Technical Report ISO/IEC 27001:2022, International Organization for Standardization, Geneva, Switzerland. Acesso em: 17 maio 2026.

Li, P., Li, S., Ding, M., Yu, J., Zhang, H., Zhou, X., and Li, J. (2022). A vulnerability detection framework for hyperledger fabric smart contracts based on dynamic and static analysis. In *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022*, EASE 2022, pages 366–374, New York, NY, USA. Association for Computing Machinery.

Liang, W., Liu, Y., Yang, C., Xie, S., Li, K., and Susilo, W. (2024). On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: A comprehensive survey. *ACM Computing Surveys*, 56(12).

Liao, Y., Kong, X., Yin, L., Zhang, G., Wang, K., Cao, Y., and Sun, X. (2026). Ds-duc: A method for data usage control in automotive supply chain based on industrial data space. *Results in Engineering*, 29.

López, A. E., Pinilla, M. A., and Mora, H. R. C. (2025). Risk-based security hardening in iot systems using owasp and cyberattack simulations. In *2025 IEEE Ninth Ecuador Technical Chapters Meeting (ETCM)*, pages 1–6. IEEE.

Nishikawa-Pacher, A. (2022). Research questions with pico: a universal mnemonic. *Publications*, 10(3):21.

Nowak, S. (2025). CORRECTION: Automating origin calculations: key considerations for manufacturers with complex supply chains. *World Customs Journal*, 19(2):138–156.

Oka, D. K. (2021). *Building Secure Cars: Assuring the Automotive Software Development Lifecycle*. John Wiley & Sons, Hoboken, NJ, USA.

OWASP Foundation (2025). OWASP Top 10:2025. https://owasp.org/Top10/2025/. Acesso em: 17 maio 2026.

Scheffel, G., Camargo, L., Sohn Junior, G., Souza, P. H. S. d., Miers, C. C., Simplicio Junior, M. A., and Pillon, M. A. (2026). UDESC-BCMX-SBSeg: Reports and supplementary material. https://github.com/udesc-bcmx-sbseg/reports. Acesso restrito, disponível mediante solicitação aos autores.

Semgrep (2026). View findings in Semgrep AppSec Platform. https://semgrep.dev/docs/semgrep-code/findings. Acesso em: 17 maio 2026.

SonarSource (2026). SonarQube Cloud: Scalable AI Code Verification. https://www.sonarsource.com/products/sonarqube/cloud/. Acesso em: 17 maio 2026.

Souza, P. H. S. d., Zachêo, J. V., Miers, C. C., Simplicio Jr., M. A., Koslovski, G. P., and Pillon, M. A. (2026). MoVChain: ESG traceability platform for the automotive supply chain. In *Proceedings of the 40th International Conference on Advanced Information Networking and Applications (AINA-2026)*, Wellington, New Zealand. Springer. April 8–10, 2026.