Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***CTI-Balanced***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Literature Review: Privacy, GDPR and Cybersecurity Issues in Cyber Threat Intelligence Sharing***

Table of Contents

Literature Review: Privacy, GDPR and Cybersecurity Issues in Cyber Threat Intelligence Sharing

Prepared for CTI-Balanced reporting to the Innovation Agency

1. Purpose and scope

This literature review supports the CTI-Balanced project requirement for a separate review of literature concerning privacy, GDPR and cybersecurity issues in the sharing of cyber threat intelligence (CTI). The review is based on bibliographic materials prepared within the project and on references drawn from project publications and related submitted work. Its purpose is not to present a full systematic literature review, but to synthesize the relevant legal, technical and organisational literature into a concise reporting document suitable for inclusion in the project documentation.

The review focuses on the central problem addressed by CTI-Balanced: how organisations can share actionable cyber threat information while maintaining compliance with data protection requirements, preserving confidentiality and integrity, and supporting secure cross-organisational cooperation. In this context, CTI sharing is treated as both a cybersecurity function and a regulated data-processing activity. The legal baseline is provided by the GDPR, the NIS2 Directive, DORA, the CER Directive, the Cyber Resilience Act and related EU cybersecurity instruments (European Parliament and Council of the European Union, 2016, 2022a, 2022b, 2022c, 2024).

The selected literature base also includes work on regulatory compliance engineering, ontology-based requirements modelling, CTI exchange in regulated sectors, MITRE ATT&CK/NIST mapping, industrial-control-system security, and semantic integration of hybrid threat intelligence (Avdeenko & Pustovalova, 2016; Hernandez et al., 2024; Kosenkov et al., 2025; Paskauskas et al., 2026; Rajamäki et al., 2024).

2. CTI sharing as a cybersecurity cooperation mechanism

Cyber threat intelligence sharing is widely understood as a mechanism for improving collective cybersecurity. It allows organisations to exchange information about incidents, indicators of compromise, malicious infrastructure, tactics, techniques and procedures, and mitigation measures. In operational terms, CTI sharing supports earlier detection, faster response, better prioritisation of security controls and improved situational awareness across sectors. In the EU regulatory context, this cooperative logic is reinforced by NIS2, which places strong emphasis on incident handling, vulnerability management, information sharing and cooperation among competent authorities and regulated entities (European Parliament and Council of the European Union, 2022a).

The cybersecurity literature also shows that CTI sharing is not merely a technical exchange of indicators. It depends on common vocabularies, standards, trust relationships, quality controls and governance mechanisms. The use of structured frameworks such as MITRE ATT&CK and mappings to the NIST Cybersecurity Framework can support a common interpretation of adversary behaviour and security functions (Al-Sada et al., 2025; Kwon et al., 2020; National Institute of Standards and Technology, 2024). In industrial and critical-infrastructure contexts, these issues are reinforced by sector-specific security

requirements, including IEC 62443 and related security-by-design approaches (ISA/IEC, 2018; Hosseini et al., 2025).

For CTI-Balanced, this implies that CTI sharing should be treated as a structured, governed process. Information must be represented in a way that supports machine processing, organisational decision-making, regulatory accountability and secure interoperability. This is why the project literature points toward semantic modelling, regulatory mapping and ontology-based approaches as useful mechanisms for aligning operational cybersecurity requirements with legal obligations (Avdeenko & Pustovalova, 2016; Guizzardi et al., 2023; Hernandez et al., 2024).

3. Privacy and GDPR issues in CTI sharing

The privacy challenge in CTI sharing arises because threat intelligence frequently contains or is derived from data that may qualify as personal data. Examples include IP addresses, email addresses, usernames, device identifiers, hostnames, traffic data, logs, geolocation data, credentials, and incident narratives that may identify employees, customers, victims or suspected threat actors. Even when the primary purpose is cybersecurity, the processing and onward sharing of such information may fall within the scope of the GDPR if an identified or identifiable natural person is involved (European Parliament and Council of the European Union, 2016).

The literature on GDPR and CTI exchange highlights a basic tension: effective cyber defence often requires timely information sharing, but data protection law requires lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Rajamäki et al. (2024), for example, address the implications of GDPR and NIS2 for CTI exchange in hospitals, a setting where cybersecurity incidents may involve sensitive operational systems and potentially identifiable individuals. This type of sectoral analysis is directly relevant to CTI-Balanced because it shows that CTI sharing must be designed around both incident-response needs and data-protection safeguards.

A GDPR-aware CTI sharing model, therefore, has to address several questions. First, it must identify the lawful basis for processing and sharing CTI data, such as legal obligation, legitimate interests, public interest or, in narrower cases, consent. Second, it must distinguish between information that is necessary for threat detection and information that creates unnecessary privacy risk. Third, it must define safeguards such as pseudonymisation, anonymisation, encryption, access restriction and role-based disclosure. Fourth, it must support breach-notification logic under Articles 33 and 34, including the distinction between notification to the supervisory authority and notification to data subjects (European Parliament and Council of the European Union, 2016; European Data Protection Board, 2024).

Recent case law and guidance also reinforce the need for careful data handling in automated or data-intensive contexts. CJEU decisions concerning automated decision-making, large-scale data retention, pseudonymisation and administrative fines are relevant because they shape the interpretation of GDPR risk, identifiability, controller responsibility and liability (Court of Justice of the European Union, 2020, 2023, 2025a, 2025b). For CTI sharing, the practical conclusion is that a privacy-preserving CTI model cannot rely on informal data exchange alone. It requires a structured representation of data categories, processing purposes, lawful bases, safeguards, responsible entities and notification pathways.

4. Cybersecurity issues in CTI sharing

The cybersecurity issues associated with CTI sharing concern the confidentiality, integrity, availability and quality of shared intelligence. CTI may itself be sensitive. If disclosed too widely, it can reveal defensive capabilities, vulnerable systems, ongoing investigations, indicators monitored by SOCs, or details of critical infrastructure. At the same time, poor-quality or unverified intelligence can create false positives, misdirect incident-response resources, or generate unnecessary operational disruption.

The literature, therefore, supports a controlled-sharing model. Secure communication channels, authentication, encryption, access control and logging are needed to ensure that CTI is shared only with authorised participants. Data integrity mechanisms are required so that recipients can trust that indicators, reports, and mitigation information have not been altered. Governance processes are also necessary to classify intelligence, manage disclosure levels, validate sources, and decide what can be shared externally. These requirements align with NIS2, DORA and the CER Directive, all of which emphasize risk management, resilience, incident reporting and security governance in regulated environments (European Parliament and Council of the European Union, 2022a, 2022b, 2022c).

Technical interoperability is another major cybersecurity issue. Standards and platforms such as STIX, TAXII, and MISP are important because they enable CTI to be exchanged in a structured, machine-readable format. Without common formats, CTI sharing remains slow, inconsistent and difficult to automate. At the same time, interoperability does not remove the need for privacy and security controls. A balanced CTI-sharing model must therefore combine standardised formats with access control, minimisation and regulatory metadata that indicate why the data is shared, under what authority, and subject to which safeguards.

The Cyber Resilience Act and related EU cybersecurity certification efforts further strengthen the view that cybersecurity obligations are moving toward lifecycle-based, security-by-design requirements for digital products and services (European Parliament and Council of the European Union, 2024; European Commission, 2024). For CTI-Balanced, this supports the need to design CTI sharing as a governed and auditable process rather than as an ad hoc exchange of technical indicators.

5. Regulatory and compliance context

The regulatory literature shows that CTI sharing sits at the intersection of several legal regimes. GDPR governs the processing of personal data; NIS2 governs cybersecurity risk management and incident reporting for essential and important entities; DORA establishes digital operational resilience requirements for the financial sector; the CER Directive addresses critical-entity resilience; and the Cyber Resilience Act introduces horizontal cybersecurity requirements for products with digital elements (European Parliament and Council of the European Union, 2016, 2022a, 2022b, 2022c, 2024).

This overlapping legal environment creates a compliance challenge. A SOC or regulated entity may need to share incident information quickly for cybersecurity purposes, while also determining whether the information includes personal data, whether a breach notification obligation has been triggered, which reporting timeframe applies, which authority must be notified, and which safeguards are required. The issue is therefore not only whether CTI can be shared, but how the sharing can be documented, justified and controlled.

Research on regulatory compliance engineering is relevant here because it addresses translating legal requirements into system requirements and operational controls. Kosenkov et al. (2025) map the requirements engineering literature on regulatory compliance, while Abualhaija et al. (2025) examine legal requirements analysis from a regulatory compliance perspective. Ontology-based and semantic approaches are also relevant because they enable the representation of legal concepts, obligations, actors, safeguards, and penalties in a structured form (Avdeenko & Pustovalova, 2016; Hernandez et al., 2024; Orlando & Santoro, 2025).

For CTI-Balanced, this regulatory context justifies a model that links legal sources to operational cybersecurity concepts. Such a model should be capable of representing regulations, requirements, incident types, reportable attributes, responsible entities, reporting timeframes, penalties, lawful bases and safeguards. This aligns with the broader direction of RegTech and automated compliance research, which increasingly treats compliance as a data- and knowledge-management problem rather than only as a manual legal review process (El Khoury et al., 2025; Imperial et al., 2025).

6. Ontology and semantic modelling as a response

The project literature provides strong support for ontology-based modelling as a means of managing the complexity of CTI sharing under privacy and cybersecurity constraints. Ontologies are useful where several domains must be connected: law, cybersecurity operations, incident reporting, organisational responsibility, data protection and technical standards. Rather than leaving these relationships implicit, an ontology can encode them as classes, properties and queryable relationships.

This approach is consistent with earlier work on ontology-based requirements engineering and regulatory mapping (Avdeenko & Pustovalova, 2016; Hernandez et al., 2024). It is also consistent with recent work on ontology-based ethicality and trustworthiness requirements, in which legal and normative concepts are formalised so they can be inspected, queried, and aligned with system design (Amaral et al., 2021; Guizzardi et al., 2023). In cybersecurity, ontology-based security-by-design work for industrial control systems further supports the use of semantic structures to organise security requirements across complex operational environments (Hosseini et al., 2025).

The CTI-Balanced literature base also connects directly to the team's existing work on semantic integration and hybrid-threat intelligence. The project publications and submitted papers emphasise the role of ontological frameworks in correlating cross-domain threat information, linking technical indicators with regulatory and operational context, and supporting more interpretable threat-intelligence workflows (Bružė et al., 2026; Paskauskas, 2025; Paskauskas et al., 2026).

In practical terms, ontology-based modelling can support privacy-preserving CTI sharing by making explicit which requirements apply, which incident types trigger reporting, which attributes may be shared, which data categories are involved, which responsible entities are accountable, which safeguards are required, and which timeframes or penalties apply. It can also support SPARQL-based validation and retrieval, allowing project partners to test whether the model correctly captures reporting chains, lawful bases, breach-notification pathways and safeguard-based exceptions.

7. Synthesis for CTI-Balanced

The reviewed literature supports four conclusions relevant to CTI-Balanced.

- First, CTI sharing is a necessary element of collective cybersecurity and resilience, especially in regulated sectors and critical-infrastructure contexts.
- Second, CTI sharing creates privacy and GDPR risks because shared cyber incident data may include personal data or information derived from personal data.
- Third, secure CTI sharing requires technical controls, common formats, governance rules, trust mechanisms and auditability.
- Fourth, ontology-based modelling provides a practical way to connect regulatory obligations with operational CTI-sharing workflows.

Accordingly, the literature supports the development of a balanced CTI-sharing model that enables actionable cybersecurity cooperation while respecting GDPR principles, breach-notification requirements, data minimisation, safeguard implementation and secure exchange. The key contribution for the project is not simply the compilation of references, but the translation of the literature into a structured compliance logic: what may be shared, for what purpose, under which legal basis, by whom, using which safeguards, within which reporting timeframe, and with which liability implications.

8. Conclusion

The CTI-Balanced literature review shows that privacy and cybersecurity cannot be treated as separate concerns in CTI sharing. CTI exchange is valuable because it improves detection, response and collective resilience, but it may also involve personal data, sensitive operational information and regulated incident-

reporting obligations. A credible CTI-sharing model therefore has to balance actionable intelligence with GDPR compliance, secure data handling, controlled disclosure, and auditability.

The reviewed sources justify the project's use of a machine-interpretable compliance model. By linking regulatory instruments, CTI-sharing requirements, incident types, reportable attributes, lawful bases, safeguards, notification paths and cybersecurity controls, the model provides a practical bridge between the literature and implementation. This directly supports the Innovation Agency's reporting requirement for a literature review addressing privacy and cybersecurity issues in CTI sharing.

9. References

Abualhaija, S., Ceci, M., & Briand, L. (2025). Legal requirements analysis: A regulatory compliance perspective. In A. Ferrari & G. Ginde (Eds.), Handbook on natural language processing for requirements engineering (pp. 209-242). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73143-3_8

Al-Sada, B., Sadighian, A., & Oligeri, G. (2025). MITRE ATT&CK: State of the art and way forward. ACM Computing Surveys, 57(1), 1-37. https://doi.org/10.1145/3687300

Amaral, G., Guizzardi, R., Guizzardi, G., & Mylopoulos, J. (2021). Trustworthiness requirements: The Pix case study. In Conceptual modeling (Lecture Notes in Computer Science, Vol. 13011, pp. 257-267). Springer. https://doi.org/10.1007/978-3-030-89022-3_21

Avdeenko, T. V., & Pustovalova, N. V. (2016). The ontology-based approach to support the requirements engineering process. In 2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE) (pp. 513-518). IEEE. https://doi.org/10.1109/APEIE.2016.7806406

Bružė, E., Paskauskas, R. A., Matulytė, R., Sabaliauskaitė, G., & Lavišius, T. (2026). Integration of hybrid threat intelligence: The HIPSTer ontological method for cross-domain correlation in influence operations. Open Research Europe, in press.

Court of Justice of the European Union. (2020). C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

Court of Justice of the European Union. (2023). C-634/21 - SCHUFA Holding. https://curia.europa.eu/juris/liste.jsf?num=C-634/21

Court of Justice of the European Union. (2025a). C-203/22 - Dun & Bradstreet Austria GmbH. https://curia.europa.eu/juris/liste.jsf?num=C-203/22

Court of Justice of the European Union. (2025b). C-413/23 P - EDPS v SRB. https://curia.europa.eu/

El Khoury, R., Alshater, M. M., & Joshipura, M. (2025). RegTech advancements: A comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting, 23(4), 1450-1485. https://doi.org/10.1108/JFRA-05-2024-0286

European Commission. (2024). Union rolling work programme for European cybersecurity certification (SWD(2024) 38 final).

European Data Protection Board. (2024). One-stop-shop case digest on security of processing and data breach notification. https://www.edpb.europa.eu/

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament and Council of the European Union. (2022a). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Parliament and Council of the European Union. (2022b). Directive (EU) 2022/2557 on the resilience of critical entities. Official Journal of the European Union, L 333, 164-198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

European Parliament and Council of the European Union. (2022c). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. Official Journal of the European Union, L 333, 1-79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). Official Journal of the European Union, L 2024/2847. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Guizzardi, R., Amaral, G., Guizzardi, G., & Mylopoulos, J. (2023). An ontology-based approach to engineering ethicality requirements. Software and Systems Modeling, 22(6), 1897-1923. https://doi.org/10.1007/s10270-023-01115-3

Hernandez, J., Golpayegani, D., & Lewis, D. (2024). Ontology-based approach for mapping concepts and requirements from regulations and standards: The case of the EU AI Act and international standards. Frontiers in Artificial Intelligence and Applications. https://doi.org/10.3233/FAIA241258

Hosseini, A. M., Kastner, W., & Sauter, T. (2025). Ontology framework supporting security-by-design of industrial control systems. IEEE Transactions on Industrial Informatics, 21(9), 7188-7197. https://doi.org/10.1109/TII.2025.3574694

Imperial, J. M., Jones, M. D., & Tayyar Madabushi, H. (2025). Standardizing intelligence: Aligning generative AI for regulatory and operational compliance. SSRN. https://doi.org/10.2139/ssrn.5146161

ISA/IEC. (2018). Security for industrial automation and control systems (ISA/IEC 62443).

Kosenkov, O., et al. (2025). Systematic mapping study on requirements engineering for regulatory compliance of software systems. Information and Software Technology, 178, 107622. https://doi.org/10.1016/j.infsof.2024.107622

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020). Cyber threat dictionary using MITRE ATT&CK matrix and NIST Cybersecurity Framework mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE. https://doi.org/10.1109/RWS50334.2020.9241271

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://www.nist.gov/cyberframework

Orlando, A., & Santoro, M. (2025). A semantic approach to understanding GDPR fines: From text to compliance insights. Computer Law & Security Review, 59, 106187. https://doi.org/10.1016/j.clsr.2025.106187

Paskauskas, R. A. (2025). A preliminary ontology for 5G network resilience: Hybrid threats, risk reduction, compliance. In 2025 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 490-497). IEEE. https://doi.org/10.1109/CSR64739.2025.11129990

Paskauskas, R. A., Bružė, E., Sabaliauskaitė, G., Matulytė, R., & Lavišius, T. (2026). Hybrid-threat intelligence: A critical review of semantic integration challenges and the role of the HIPSTer ontological framework. Journal of Intelligent Communication, in press.

Rajamäki, J., et al. (2024). Implications of GDPR and NIS2 for cyber threat intelligence exchange in hospitals. WSEAS Transactions on Computers, 23, 1-11. https://doi.org/10.37394/23205.2024.23.1

Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv. https://doi.org/10.48550/arXiv.2412.08084

Appendix A. Targeted 2025–2026 Web of Science update search

A.1 Purpose of the update search

A targeted update search was conducted in Web of Science to assess whether recent literature from 2025–2026 materially adds to the CTI-Balanced literature review on privacy, GDPR/data protection issues, confidentiality, cybersecurity safeguards, and cyber threat intelligence (CTI) sharing.

The purpose of this search was not to conduct a full systematic literature review. Rather, it was used as a proportionate freshness check to confirm whether the project's existing literature base remains current and whether any recent publications should be noted as supplementary evidence.

A.2 Search process

The search was conducted using the Web of Science Query Builder.

Database/platform: Web of Science
Search interface: Query Builder
Date searched: 29 April 2026
Publication years: 2025–2026
Initial results: more than 800 records
Records retained/exported for review: 19 records

Purpose of screening: to identify recent publications relevant to CTI sharing, privacy-preserving exchange, GDPR/data-protection implications, confidentiality, secure dissemination, trust frameworks, access control, interoperability, and cybersecurity safeguards.

A.3 Search string

The following Boolean search string was used as the basis for the update search:

TS=(("cyber threat intelligence" OR CTI) AND (sharing OR exchange OR dissemination) AND (privacy OR GDPR OR "data protection" OR confidentiality OR "personal data"))

The search results were then manually screened to retain articles that were clearly relevant to CTI sharing and included at least one of the following themes: privacy-preserving exchange, secure CTI dissemination, confidentiality, trust, access control, federated learning, blockchain/distributed architectures, STIX/TAXII-compatible sharing, or cybersecurity situational awareness.

A.4 Summary of findings

The targeted update search confirms that recent literature continues to emphasise the same core issues identified in the main CTI-Balanced literature review. Recent work treats CTI sharing as an important mechanism for improving cyber situational awareness, incident response, and cross-organisational resilience. However, the literature also confirms that CTI sharing remains constrained by concerns over privacy, confidentiality, trust, access control, data ownership, and the possible exposure of sensitive incident-related information.

Several of the recent publications focus on technical mechanisms for privacy-preserving or trusted CTI sharing. These include blockchain-based approaches, Hyperledger/IPFS-based architectures, federated learning, automated STIX-compatible dissemination, and access-control mechanisms designed to support controlled disclosure of threat intelligence. The additional retained records further reinforce the prominence of federated

and privacy-preserving approaches, including inference-risk mitigation, private set intersection, and cross-border federated cybersecurity architectures.

Other sources address incentive structures, interoperability, advanced persistent threat datasets, and the need for secure and scalable CTI-sharing frameworks. Overall, the updated search does not materially change the conclusions of the main literature review. Instead, it strengthens them. The recent literature reinforces the need for a balanced CTI-sharing model that enables timely and actionable exchange of cyber threat intelligence while preserving privacy, confidentiality, data-protection safeguards, and cybersecurity controls.

A.5 Relevance to the CTI-Balanced literature review

The update search supports three conclusions relevant to CTI-Balanced.

First, privacy and confidentiality remain central concerns in CTI sharing. Recent CTI-sharing frameworks continue to address the risk that shared intelligence may contain sensitive organisational information, personal data, network identifiers, incident details, or operationally sensitive indicators.

Second, secure and trusted sharing architectures are increasingly important. The recent literature gives particular attention to federated, decentralised, blockchain-based, and access-controlled architectures that seek to reduce reliance on centralised CTI repositories and to give data owners greater control over how threat intelligence is shared.

Third, interoperability remains a practical requirement. Several recent works continue to rely on or refer to structured CTI formats and exchange mechanisms, including STIX and TAXII. This confirms the relevance of modelling CTI-sharing requirements in a structured and machine-interpretable form, as pursued in the CTI-Balanced ontology work.

For these reasons, the update search should be treated as supplementary support for the main literature review rather than as a separate systematic review.

A.6 References for Appendix A

Ali, H., Buchanan, W. J., Ahmad, J., Abubakar, M., Khan, M. S., & Wadhaj, I. (2025). TrustShare: Secure and trusted blockchain framework for threat intelligence sharing. Future Internet, 17(7). https://doi.org/10.3390/fi17070289

Arikkat, D. R., Cihangiroglu, M., Conti, M., Rehiman, K. A. R., Nicolazzo, S., Nocera, A., & Vinod, P. (2025). SeCTIS: A framework to secure CTI sharing. Future Generation Computer Systems, 164. https://doi.org/10.1016/j.future.2024.107562

Arshad, M. Z., & Algarni, A. (2026). HoloCyberChain: A distributed entropy-fingerprint blockchain for global cyber threat intelligence. AIP Advances, 16(2). https://doi.org/10.1063/5.0317223

Bouharoun, M., & Erradi, M. (2025). FLAIR: A federated learning approach against inference attacks and risks. In M. Al-kfairy, M. Aldwairi, K. Choo, M. Tubishat, S. Alrabaee, & O. Alfandi (Eds.), Security and Privacy in Social Networks and Big Data, SocialSec 2024 (Vol. 15565, pp. 138–156). Springer. https://doi.org/10.1007/978-981-96-3774-4_9

El Haddouti, S., Lazraq, W., Loven, L., El Kettani, M. D. E.-C., & Chaoui, H. (2026). A holistic framework for privacy-preserving and trusted cyber threat intelligence in Industry 5.0: A fusion of blockchain and tiny semi-supervised class-incremental learning with catastrophic forgetting mitigation. Internet of Things, 37. https://doi.org/10.1016/j.iot.2026.101899

Gambo, M. D., Khan, A. H., Almulhem, A., & Almadani, B. (2025). An efficient framework for automated cyber threat intelligence sharing. Electronics, 14(20). https://doi.org/10.3390/electronics14204045

Ikegwu, A. C., Nnabue, J. C., Kinse, A. S., & Alo, U. R. (2025). A survey of cyber threat intelligence in embedded system driven security for mobile health systems. Journal of Cloud Computing: Advances, Systems and Applications, 15(1). https://doi.org/10.1186/s13677-025-00811-3

Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., & Al-Betar, M. A. (2025). Federated conditional variational auto encoders for cyber threat intelligence: Tackling non-IID data in SDN environments. IEEE Access, 13, 26273–26288. https://doi.org/10.1109/ACCESS.2025.3529894

Messinis, S., Protonotarios, N. E., Kalogerasi, D., & Doulamisi, N. (2025). Threshold multiparty private set intersection via federated graph neural networks. In I. Praca, S. Bernardi, & P. Inacio (Eds.), Cybersecurity, EICC 2025 (Vol. 2500, pp. 356–371). Springer. https://doi.org/10.1007/978-3-031-94855-8_23

Mrabet, M. (2025). TrustFed-CTI: A trust-aware federated learning framework for privacy-preserving cyber threat intelligence sharing across distributed organizations. Future Internet, 17(11). https://doi.org/10.3390/fi17110512

Peratikou, A., Charalambous, E., Smyrli, P., & Stavrou, S. (2025). ATHENA: A federated architecture for cross-border cybersecurity operations and situational awareness. 2025 IEEE International Conference on Cyber Security and Resilience, 1043–1048. https://doi.org/10.1109/CSR64739.2025.11129994

Rahman, S., Pal, S., Jadidi, Z., & Karmakar, C. (2025). Robust cyber threat intelligence sharing using federated learning for smart grids. IEEE Transactions on Computational Social Systems, 12(2), 635–644. https://doi.org/10.1109/TCSS.2024.3496746

Reittinger, T., Grill, J., & Pernul, G. (2026). Share and benefit: Incentives for cyber threat intelligence sharing. International Journal of Information Security, 25(1). https://doi.org/10.1007/s10207-025-01165-2

Ren, B. (2025). Security and privacy challenges in 5G core AI-powered threat detection and mitigation strategies. Internet Technology Letters, 8(5). https://doi.org/10.1002/itl2.70070

Siddique, M. M., Galib, S. M., Adnan, M. N., & Sheikh, M. N. A. (2026). DFedForest++: A novel privacy-enhanced framework for integrating cyber threat intelligence in IDS using federated learning. Future Internet, 18(3). https://doi.org/10.3390/fi18030173

Syed, A., Nour, B., Pourzandi, M., Assi, C., & Debbabi, M. (2025). Comprehensive advanced persistent threats dataset. IEEE Networking Letters, 7(2), 150–154. https://doi.org/10.1109/LNET.2025.3551989

Tolah, A. (2025). BlockIntelChain: A blockchain-based cyber threat intelligence sharing architecture. Scientific Reports, 16(1). https://doi.org/10.1038/s41598-025-29152-6

Tom, A. K., Khraisat, A., Jan, T., Whaiduzzaman, M., Nguyen, T. D., & Alazab, A. (2025). Survey of federated learning for cyber threat intelligence in Industrial IoT: Techniques, applications and deployment models. Future Internet, 17(9). https://doi.org/10.3390/fi17090409

Venckauskas, A., Toldinas, J., Morkevicius, N., Serkovas, E., & Kristaponis, M. (2025). Enhancing the resilience of a federated learning global model using client model benchmark validation. Electronics, 14(6). https://doi.org/10.3390/electronics14061215

Editor
<<Main Editor>>

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Disclaimer