SMAUG

Funded by the European Union

Policy Brief°

AI, Data Governance and Cloud Cybersecurity in Maritime Surveillance

Annalisa Triggiano – Daisy Romanini***

1. Background

Maritime security is crucial for safeguarding oceans, coasts, and ports from threats that could disrupt trade and global stability. It ensures the safety of all activities at sea, including border defense, the protection of critical infrastructure, and the prevention of environmental crimes. Numerous challenges to maritime security exist, including piracy, terrorism, illegal fishing, smuggling, human trafficking, and environmental offences. Addressing these threats requires collaboration and vigilance from national and international entities, such as military forces, coast guards, governments, and private security firms. These groups work together to keep shipping lanes operational, ensure the safe movement of goods and people, and enforce laws that protect economic and environmental well-being. Their efforts include:

- Advanced tracking systems to monitor vessels in real-time and detect suspicious activities
- Rapid-response mechanisms to address issues promptly.
- Comprehensive regulations to maintain a secure and lawful maritime domain.

To support cleaner, safer, and modern shipping in the EU, in November 2024 the Council of Europe adopted, among others, four new pieces of legislation of the so-called Maritime Safety's legislative

° This policy brief is the result of an interdisciplinary dialogue between researchers that took the opportunity to share methods and knowledge in the context of the release of the D2.1. Report on Data Governance, under the WP2 of the SMAUG EU Funded project (GA:101121129) and seminars organized within the LIDER Lab research activities, Scuola Superiore Sant'Anna, Pisa (www.lider-lab.it).

* PostDoc researcher Scuola Superiore Sant'Anna, Pisa – Italy is responsible of §1, 2, 3 and co-authored §5.

** PhD Candidate IMT Alti Studi Lucca, Italy is responsible of § 4, and co-authored §5 under the supervision of M. Petrocchi, Istituto di Informatica e Telematica CNR and IMT Scuola Alti Studi Lucca.

package, two of which are particularly relevant for SMAUG purposes, namely those amending the relevant directives on:

- the investigation of accidents in the maritime transport sector;
- the ship-source pollution;
- the compliance with flag state requirements;
- the port state control

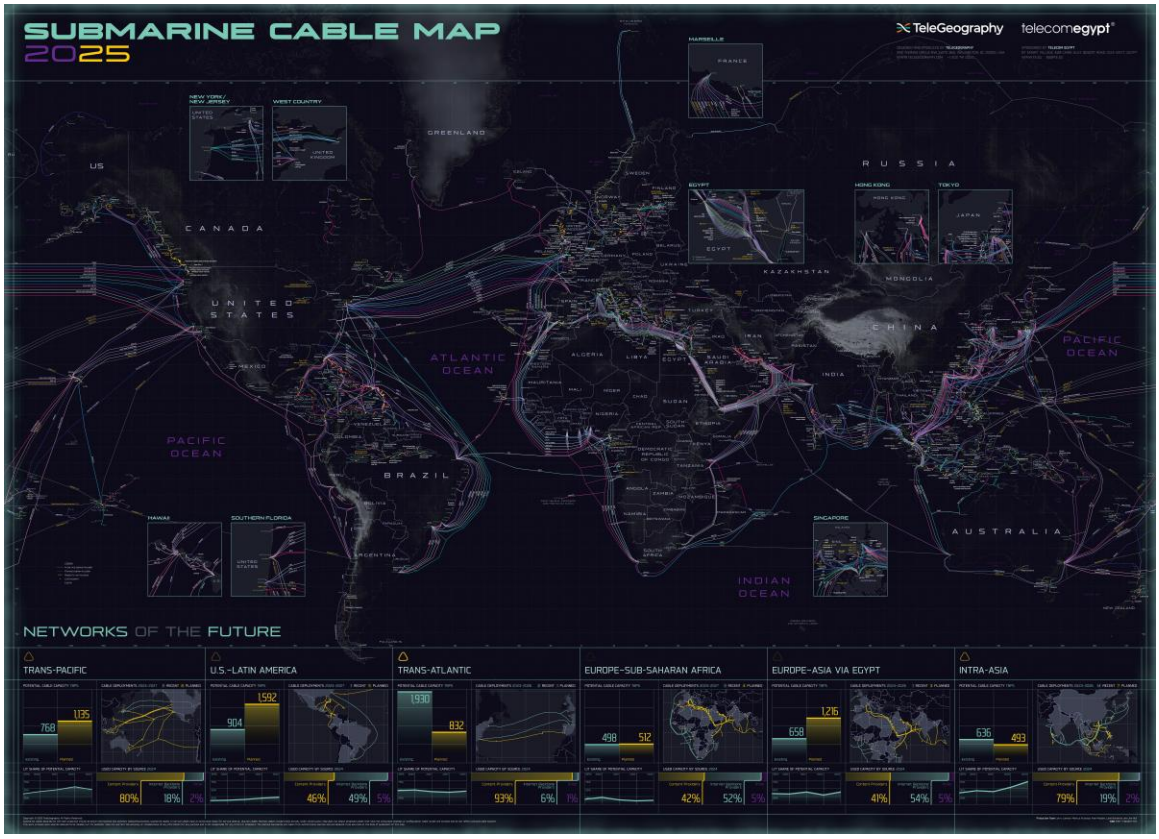
A very large amount of data is produced regarding maritime activities, marine environment, or weather monitoring (maritime surface/underwater, air, remote-piloted air systems (RPAS), satellite, civil administration, military, leisure and tourism actors, marine research and monitoring, extraction, shipping industry, non-governmental organizations). Herewith it is necessary to provide a short review of the current state of underwater surveillance, with a focus on the progress made in each of these research domains and on the data issues emerging from the research itself and the future use of surveillance technologies according to EU Legislative Framework. This policy paper examines shortly the regulatory and technological frameworks governing data in the Smart Maritime and Underwater Guardian (SMAUG) Project. It highlights key legal considerations, the role of artificial intelligence (AI) in surveillance, and cross-border data sharing policies under the European Union's legislative framework for security purposes. This policy paper may also aim to provide policymakers and researchers with insights into optimizing data governance while maintaining compliance with regulatory requirements. Special emphasis is given to the challenges posed by AI-driven maritime surveillance and the necessity of harmonizing regulatory compliance across multiple EU frameworks. Those below are, for example, key issues:

• The maritime domain is experiencing a rapid digital transformation, characterized by the adoption of AI-driven surveillance systems, remote-piloted air systems (RPAS), and autonomous underwater vehicles (AUVs).
• These advancements generate vast amounts of data, necessitating a robust data governance structure to ensure compliance with regulatory constraints. The SMAUG project addresses this challenge by developing an integrated maritime security system that enhances underwater threat detection through AI and data-driven methodologies

2. Some Highlights: Maritime Security and Underwater Detection

The SMAUG project aims to enhance maritime security by integrating diverse surveillance technologies with a focus on AI-based threat detection. This will happen through a combination of AI analysis of various sensor data sources, and underwater and surface threat detection will be changed from a manual labour-intensive operation to an automated, notification-based system.

Today, over 80% of world trade is conducted by sea, and the continuous movement of vessels requires port security processes to be robust and effective, especially for monitoring and detecting legal and illegal activities at ports, in coastal areas and on borders. Geopolitical tensions are also turning the bottom of the oceans into sensitive terrain that needs to be protected. Let's consider, for example, the most relevant critical infrastructures, the submarine cables: the new edition of Submarine Cable Maps (2025) depicts 597 cable systems and 1,712 landings that are currently active or under construction:



Source: https://submarine-cable-map-2025.telegeography.com/

Europe is actively committed in defending submarine cables, as they play a crucial role in modern economy. The security of the EU's submarine cable infrastructure must be significantly enhanced, as it has been underlined in EU recent (21.02.2025) Joint Communication [JOIN(2025) 9 final] representing an EU Plan on Cable Security. The Joint Communication presents strong actions in a whole resilience cycle approach: prevent, detect, respond and repair, and deter. The EU must first prevent disruptive incidents and increase its resilience against the threats and vulnerabilities of submarine cable infrastructures. It must also increase its detection capacity to be in position to identify and anticipate threats as early as possible. When an incident occurs, the EU must increase its capacity to respond in a coordinated way and in solidarity with the Member States most affected. In particular, the EU must develop the right capacities to recover as quickly as possible from any incident. Finally, the EU must enhance its deterrence posture. It will act to protect the security of critical maritime infrastructure and hold malicious actors accountable, including actions against the 'shadow fleet'.

The primary goal of SMAUG project is properly to improve the underwater detection of threats in ports and their entrance routes, by means of an integrated system capable of providing data concerning threat analysis between 3 main elements:

• ports security infrastructure
• advanced underwater detection systems
• surveillance vessels

Within this context, the SMAUG project seeks to detect, track and monitor potentially illegal and harmful movements and products entering EU ports and coasts by means of an integrated system which combines security management, advanced underwater detection systems and surveillance vessels. More specifically, underwater threats are detected and located using four main methods. The first method is acoustic detection, in which a series of hydrophones listen for sounds emitted by small autonomous underwater vehicles. Secondly, a sonar performs a quick scan of the hull and the bottom of the harbor. The third method of underwater detection is high-resolution sonar inspection, which is used to inspect objects in water with poor visibility. Finally, collective autonomous location is employed, whereby a coordinated swarm of autonomous underwater vehicles act cooperatively.

These systems, supported by artificial intelligence, can more effectively detect unlawful and dangerous goods and/or threats hidden beneath the surface of the water. SMAUG will thus make a significant contribution to maritime security by improving the protection of infrastructures and vessels and the detection of vessels, including narco-submarines, suspected of conducting illegal or potentially dangerous activities. The combination of these tools will allow SMAUG to prompt solutions capable of detecting possible threats to infrastructure or vessels, as well as identify vessels with concealed goods.

3. Data governance and AI-based Maritime Surveillance Tools

The dramatic increase in digital technologies in the maritime sector raises the question of the cybersecurity to be maintained. The role of artificial intelligence will be to protect systems against cyber-attacks. This is achieved by rapidly processing large quantities of data, and then identifying patterns of abnormal behavior or vulnerabilities within this organized data. The integration of AI in the maritime industry raises multiple safety challenges, starting with the governance of data. Data on which AI relies to perform its task reliably. The "quality" and "distortion" of data, the margin of error in its interpretation and the possibility of cyber threats are all crucial issues associated with maritime AI. In the face of all this, it is above all essential to maintain human expertise to oversee it all.

Data sharing even among European maritime authorities and ports presents, furthermore, complexities due to data sensitivity, security threats, and interoperability issues. The primary challenges include the fact that Surveillance Tools must be compliant with European Technological Frameworks, and namely:

• Data Privacy and Security: Ensuring compliance with GDPR while sharing sensitive surveillance data.
• Interoperability and Standardization: Achieving seamless data exchange between national and international maritime agencies
• Cybersecurity Risks: Protecting critical maritime infrastructure from cyber threats
• Legal and Ethical Considerations: Balancing security needs with privacy rights and regulatory compliance.

Ensuring that maritime surveillance systems comply with ethical AI principles is another crucial challenge. Ethical considerations and privacy concerns deserve particular attention when it comes to data collection and monitoring. Since AI systems are built using data gathering, from example, from satellite sensors, this can lead to excessive monitoring, including unlawful intrusion into the private and professional lives of those operating in these areas. In the event of a hack, cybercriminals could also gain access to the data collected, compromising not only privacy but also the security of maritime operations. The question of system autonomy is also being discussed. This dimension complicates and slows down the creation of standards around the various applications of AI in the maritime industry. Standards that are nonetheless essential to the proper deployment of AI. By harnessing the power of AI, the maritime industry can move towards a safer, more sustainable and more efficient future. However, it is crucial to address the challenges associated with AI implementation to ensure it aligns with international standards and human rights principles. AI models used for threat detection must be trained on unbiased datasets to avoid discriminatory practices in surveillance operations.

Nevertheless, ensuring cross-sector collaboration among EU maritime security agencies requires standardized protocols for secure data transmission. Data sources for sustainable maritime surveillance can be categorized, according to some scholars, into three distinct groups: sensors, predefined databases, and publicly accessible internet sources[1]. Nonetheless, conducting maritime surveillance using these data sources may present several challenges, not mentioned above, including the technical capabilities of the data sources, the vastness of the maritime areas to be monitored, the variability of the image on the sea surface owing to factors such as waves, surface currents and wake, weather events such as precipitation and cloud density, limited visibility at night and in foggy weather, traffic density of the area to be monitored, and detection of diverse vessel types and sizes[2]. In order to discern maritime irregularity with the aid of artificial intelligence, the normal situation must first be fully comprehended and modelled in a way that can be used in artificial intelligence applications.

[1] Stróżyna, M.; Abramowicz, W.; Węcel, K.; Filipiak, D.; Małyszko, J. *Data Analysis in the Maritime Domain*; PUEB Press: Poznan, Poland, 2022, Data analysis in the maritime domain

[2] Bloisi, D.D.; Previtali, F.; Pennisi, A.; Nardi, D.; Fiorini, M. Enhancing Automatic Maritime Surveillance Systems with Visual Information. *IEEE Trans. Intell. Transp. Syst.* 2017, *18*, 824–833, Enhancing Automatic Maritime Surveillance Systems With Visual Information | IEEE Journals & Magazine | IEEE Xplore

In SMAUG Scenario the anomalies below the water surface will be identified by automatically assessing threats to ships at harbor's entrances and within piers. How? Scanning a region of interest. Then it will be necessary to proceed to data collection (Raw information from SMAUG devices). Then it will come the time for AI Processing (activity dealing with Raw Data processing to extract valuable insights, like alerts, or notification). The processed data is then fed int the SMAUG DSS to assist final decision-making (Decision Support phase). All insights and model decisions are then displayed in on the SMAUG (Visualization). The Rapid Sonar Hull Scan may present some issues in data collections. First of all, there is, regarding acoustic detection in general, a lack of historical hydrophone data to train the System. Secondly, the detection on vertical surfaces may present unexpected problems, due to the fact that both physical data collection and/or the algorithm could struggle with vertical surfaces. Another difficulty may arise from the fully-automatic detection, which makes mandatory a post processing activity.

Effective data governance in this research context requires the regulation of data collection, processing, and sharing. Governing the Data flows in SMAUG Project is one of the tasks of SSSA and SmartLex. This activity is crucial and illustrates the legal and ethical constraints in cross-border data sharing, mapping the strategy for data governance mechanisms. A special focus has been given on the need for data pseudonymization/anonymization, since AI-driven tools enhance threat detection and situational awareness but raise concerns about:

• Data Minimization and Pseudonymization: Ensuring AI systems comply with GDPR by implementing pseudonymization techniques. One of the major concerns in maritime data governance is ensuring that sensitive data, including personally identifiable information (PII) and classified security data, remains protected while facilitating cross-border collaboration. The GDPR plays a significant role in defining how personal data should be handled within SMAUG, ensuring that AI-based surveillance adheres to data protection principles, including transparency, fairness, and accountability. At this purpose, SmartLex has created and is testing an intelligent pseudonymization tool for secure data sharing: the main purpose is to address the challenges of manual pseudonymization, a crucial yet costly, labor-intensive, and time-consuming process for ensuring privacy protection in data dissemination. By automating this process, the project will significantly accelerate pseudonymization and facilitate compliance with GDPR regulations regarding the secondary use of personal data, even if, however, the final responsibility for verifying the level of pseudonymization remains with the user. The key challenge for this pseudonymization

tool is to strike a balance between effective anonymization and preserving the meaning and usability of the data.

Key legislative frameworks impacting data governance analysis in Research Projects dealing with Maritime Security (like SMAUG) should so include, so far, the following assessment:

• General Data Protection Regulation (GDPR)
• Data Governance Act (DGA) & Data Act
• Artificial Intelligence Act (AI Act)
• Cyber Resilience Act & Cyber Solidarity Act
• NIS2 Directive
• AI Act

Moreover, under the AI Act, high-risk AI systems, such as those used in border and security surveillance, must adhere to strict guidelines regarding fairness, transparency, and accountability. It is necessary to take into account these risks and possible solutions:

- Bias and Accountability in AI Decision-Making: Establishing ethical frameworks to mitigate biases in AI-driven security assessments.
- Automated Decision-Making Risks: Addressing transparency and accountability in AI-based maritime threat analysis.

In this context, a relevant role is played by cloud services to set how digital assets could be securely shared in the given scenarios with common and standardized paths of certification.

4. Certifications in European Cloud Cybersecurity

In light of the growing reliance on digital tools (particularly AI and cloud services) for maritime security and surveillance, ensuring trust and accountability in cloud-based infrastructures becomes a critical concern. As data is increasingly processed and shared across borders, secure and standardized cloud certification frameworks are needed to support both operational effectiveness and legal compliance within the EU.

The need to move away from fragmented and non-standardized cloud regulations has become increasingly evident in recent years. Governments have recognized the benefits of embracing cloud computing as a universal innovation tool, capable of delivering high-quality solutions for both

governmental administrations and citizens, while also serving as an economic catalyst. To fully harness this potential, it is vital to establish effective governance, policies and regulations that guarantee data accountability for businesses, especially small and medium-sized enterprises, as well as government entities[3]. Additionally, these measures should encourage cross-border data transfers, even among regions with varying data privacy rules. Nonetheless, internationally recognized standards, non-binding certifications and best practices can play a pivotal role in ensuring consistency across regulatory frameworks.

It is essential to acknowledge the ongoing challenge of regulatory fragmentation within the cloud computing landscape, as this issue significantly impacts scalability for both cloud providers and their customers. A potential future contribution to this area could involve a more in-depth analysis of how EU legislation and certifications apply to different cloud service models (IaaS, PaaS and SaaS) as well as various cloud deployment types, including public clouds, private clouds, hybrid clouds and sovereign clouds. Each of these models and types presents unique regulatory challenges and compliance requirements, which can affect supply chains differently[4]. For instance, the implications of GDPR compliance may vary significantly between a public cloud service provider and a private cloud solution tailored for a specific organization.

As new legislative initiatives emerge, each introduces its own framework, which can inadvertently complicate the regulatory environment. Therefore, it is crucial to harmonize these frameworks to avoid creating additional challenges. In this context, the EU Cloud Code of Conduct serves as a pivotal reference point for upcoming projects on cloud regulation. To address this concern effectively, understanding how these regulations interact can reveal whether they collectively contribute to a coherent framework or exacerbate fragmentation. For example, while the EU Cloud Code of Conduct aims to enforce GDPR compliance, its applicability and effectiveness may differ across cloud service models and types, necessitating a tailored approach to compliance strategies.

In 2021, the European Commission launched the "*2030 Digital Compass: The European way for the Digital Decade*", a strategic framework aimed at guiding Europe's digital transformation. This

[3] Khatri, V.; Brown, C. V. *Designing data governance*. Communications of the ACM, 2010, 53 (1), 148-152. Designing data governance | Communications of the ACM

[4] Wallis, T.; Johnson, C. *Implementing the NIS Directive, driving cybersecurity improvements for Essential Services*. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, 1-10, Dublin: IEEE. (PDF) Implementing the NIS Directive, driving cybersecurity improvements for Essential Services

initiative sets a goal for at least 90% of small and medium-sized enterprises to reach a basic level of digital engagement by 2030.[5] However, SMEs face substantial challenges in their digital transformation efforts; in 2021, only 55% had achieved this level of engagement, compared to 88% of large corporations. The disparity is particularly evident in cloud service utilization (40% for SMEs versus 72% for large enterprises) and artificial intelligence adoption (7% versus 28%)[6].

To manage the complexities of cloud computing, SMEs commonly use various cloud storage and file-sharing solutions, such as Microsoft Office 365, Google Drive and Amazon Web Services (AWS). While these services offer many benefits, they also pose privacy and security risks, especially for businesses that handle personal or sensitive data. To mitigate these risks, EU policies and international standards have been established, including certifications like the ISO/IEC 27000 series and the European Cybersecurity Certification Scheme for Cloud Services (EUCS). These certifications assist cloud providers in demonstrating their commitment to data security and privacy, thereby reassuring SMEs and other organizations that their data is being managed responsibly. By adhering to these standards, cloud providers can help close the digital engagement gap between SMEs and large enterprises, allowing more businesses to reap the benefits of cloud computing while addressing associated risks.

4.1 ISO/IEC 27000 Series

The Information Security Management Systems (ISMS) standards family, also known as the ISO/IEC 27000 series, comprises a collection of information security standards that can be combined to create an internationally recognized framework grounded in industry practices. This set of standards enables any organization (e.g. commercial enterprises, government agencies, not-

[5] The Communication, released on March 9, 2021, suggests establishing a collection of digital guidelines, swiftly initiating significant multinational initiatives and formulating a legislative suggestion outlining a strong governance structure to oversee advancements – referred to as the *Digital Compass*. Retrieved from: 2030 Digital Compass: the European way for the Digital Decade - EU4Digital

[6] European Commission. *2030 Digital Compass: the European way for the Digital Decade*. 2021. Retrieved from: Digital decade

for-profit organizations) to efficiently manage the security of their information, including financial data, intellectual property, employee records, or data entrusted to them by external parties[7].

The primary standards related to cloud-based environment protection and security incident risk management are:

- ISO/IEC 27001:2022: An international benchmark for information security management systems, providing guidance on establishing, executing, sustaining and continually enhancing an information security management system. Adhering to ISO 27001 means that an organization has established a framework for enhancing cyber resilience and mitigating risks linked to data security, promoting a holistic approach to safeguarding information.
- ISO/IEC 27017:2015: Provides specific guidance for cloud service security measures, incorporating ISO 27001 standards within a cloud computing context. It serves as an advisory resource for cloud service providers in establishing protective measures for their customers, helping to protect information assets within the cloud environment, comply with legal and regulatory requirements and reduce the risk of information security incidents.
- ISO/IEC 27018:2019: Outlines regulatory requirements for the protection of Personally Identifiable Information (PII) in the cloud. It offers recommendations for safeguarding personal data stored in the cloud and helps organizations demonstrate adherence to data protection rules, thereby enhancing security and fostering trust between organizations and their customers.

While the ISO/IEC 27000 series provides a comprehensive framework for information security management, a critical assessment reveals potential challenges in its application to cloud services. ISO 27001 establishes the criteria for an information security management system that employs a risk-focused approach to protect information, encompassing individuals, processes and technology. In comparison, ISO 27017 and ISO 27018 are not management system standards, so certification cannot be achieved for them directly. However, their security measures can be incorporated into an ISMS that complies with ISO 27001, enabling a company to attain independently validated

[7] International Organization for Standardization. *ISO/IEC 27000 family. Information security management*, 2022. Retrieved from: ISO - ISO/IEC 27000 family — Information security management

certification as evidence of its conformity to that specific standard. However, the standards' ability to address the unique security considerations of cloud computing is not sufficiently explored[8].

One key concern is the standards' adaptability to the rapidly evolving cloud computing landscape. As new cloud technologies and deployment models emerge, the ISO/IEC 27000 series may struggle to keep pace with the changing security requirements[9].

Furthermore, the standards' effectiveness in addressing the shared responsibility model between cloud providers and customers is not clearly established. In a cloud environment, security responsibilities are shared between these parties, and the standards do not adequately define their respective roles. This ambiguity can lead to confusion and gaps in the implementation of security measures[10].

Another issue is the standards' ability to provide clear guidance on incident response and reporting in cloud environments. As previously mentioned with the NIS1 Directive, when a security incident occurs in a cloud environment, it may affect multiple customers simultaneously. The standards do not address how cloud providers should handle such scenarios, particularly in terms of notifying affected customers and relevant authorities[11].

In conclusion, the standards should offer more specific guidance on implementing their requirements in cloud environments, clarifying the shared responsibility model and defining clear roles and obligations for cloud providers and customers. By addressing these cloud-specific considerations, the ISO/IEC 27000 series can more effectively enhance the security of cloud services and promote a secure and resilient digital ecosystem.

---

[8] Kamara, I. *European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience*. Innovation: The European Journal of Social Science Research, 2024, 1-20. Full article: European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience

[9] Almorsy, M.; Grundy, J.; Müller, I. *An Analysis of the Cloud Computing Security Problem.* APSEC 2010 Cloud Workshop, 2010, 1-6, Sidney: IEEE. [1609.01107] An Analysis of the Cloud Computing Security Problem

[10] Hashizume, K.; Rosado, D.; Fernández-Medina, E.; Fernandez , E. B. *An analysis of security issues for cloud computing.* Journal of Internet Services and Applications, 2013, 4(5), 1-13. An analysis of security issues for cloud computing | Journal of Internet Services and Applications | Full Text

[11] Zissis, D.; Lekkas, D. *Addressing cloud computing security issues*. Future Generation Computer Systems, 2012, 28 (3), 583-592. Addressing cloud computing security issues - ScienceDirect

4.2 European Cybersecurity Certification Scheme for Cloud Services (EUCS)

The ISO/IEC 27000 series offers a strong foundation for security controls but falls short of the depth required by the European Cybersecurity Certification Scheme for Cloud Services (EUCS)[12]. Although the EUCS control structure heavily draws from ISO standards, it has been refined with more specific criteria aligned with different assurance levels. These criteria, developed based on prevailing European practices and insights from documents released by Member States managing National Schemes for cloud services, such as France's "SecNumCloud" certification[13], were facilitated by a dedicated task force within the European Union Agency for Cybersecurity (ENISA), including representatives from companies such as SAP, Deutsche Telekom's T-Systems, Cisco, and Amazon[14].

Released as a draft in December 2020, the proposed framework poses a significant challenge for Cloud Service Providers (CSPs). It surpasses the information security controls outlined in the ISO 27001 standard, which underpins the technical assurances specified in the EU Cloud Code of Conduct[15]. Unlike traditional cloud service models (SaaS, PaaS and IaaS), the EUCS assesses the effectiveness of controls based on specific capabilities offered by cloud services across three assurance levels:

1. Basic level: Ensures a cloud service meets security requirements, providing assurances against known risks of attacks and incidents.
2. Substantial level: Ensures a cloud service meets security requirements, providing assurances against known risks and attacks by individuals with limited skills and resources.

[12] European Union Agency for Cybersecurity. *EUCS - Cloud Services Scheme*. 2020. Retrieved from: EUCS – Cloud Services Scheme | ENISA

[13] The SecNumCloud requirements repository consists of a set of guidelines that are applicable to cloud service providers seeking to either validate the services they offer or adhere to security recommendations established by the French agency ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). The requirements outlined in the SecNumCloud repository serve as safeguards to prevent customer data access by cloud service providers subject to non-European regulations. These requirements encompass a combination of legal, operational and technical measures. Retrieved from: anssi_Recommendations on hosting sensitive IS in the cloud.pdf

[14] Agnello, D.; Sica, A. V. *Le nuove certificazioni cloud europee: cosa sono e perché preoccupano le big-tech*. 2022. Retrieved from: Le nuove certificazioni cloud europee: cosa sono e perché preoccupano le big-tech - Agenda Digitale

[15] EU Cloud CoC. *EU Cloud Code of Conduct (CoC)*. 2022. Retrieved from: EU Cloud CoC: EU Cloud CoC

3. High level: Ensures a cloud service meets security requirements, providing assurances against both known and potential risks, including attacks by individuals with significant skills and resources.

ENISA recommends service types for each assurance level: basic for non-critical data, substantial for critical business data, and high for critical mission services, such as airline application services.

The scheme is voluntary, offering triennial and renewable certification across all EU member countries. It covers all cloud service types, from infrastructure to applications, aiming to build trust and establish security requirements as standard references. However, adoption of the EUCS is not mandatory, though it may become a de facto requirement in highly regulated sectors like financial services or healthcare[16].

While the EUCS appears to have gained significance as a key EU tool for enhancing cybersecurity protection, its integration into existing cloud services has not received adequate attention. This is expected to change when regulators transition to the EUCS in the future. However, this does not imply that widespread integration is imminent. In fact, a 2020 ENISA survey revealed that 62% of regulatory bodies had no intention of adopting this framework, while 25% had intentions but no immediate plans, as they had not allocated resources for this purpose. Only 12% of organizations had strategized the transition and set aside funds for it[17]. The challenge lies in addressing a wide range of stakeholders in the market, a continually evolving landscape of cloud services, and the presence of various systems within the Member States. The ultimate objective is to present the EUCS project as a comprehensive technological system that offers cybersecurity assurances across the entire cloud supply chain, categorized into three levels: basic, substantial, and high. This strategic plan aims to facilitate a shift from the current national systems to a unified community regulatory framework.

Table 1 summarizes the main European security certification schemes and their targets.

[16] Kamara, I.; Leenes, R.; Stuurman, C.; van den Boom, J. *The cybersecurity certification landscape in the Netherlands after the Union*. Tilburg: National Cyber Security Centre of the Netherlands, 2020. Retrieved from: The cybersecurity certification landscape in the Netherlands after the Union Cybersecurity Act - Tilburg University Research Portal

[17] Ganzaroli, A.; Marinos, L.; Nasi, G.; Pasic, A.; Portesi, S. *Cloud Cybersecurity Market Analysis*. 2020. Retrieved from: Cloud Cybersecurity Market Analysis | ENISA

ISO/IEC 27001:2022	ISO/IEC 27017:2015	ISO/IEC 27018:2019	EUCS (2020)
It ensures enterprises have established a framework for enhancing cyber resilience and mitigating risks linked to the security of data they own or handle.	It helps organizations to protect their information assets within the cloud computing environment, comply with legal and regulatory requirements, reduce the risk of information security incidents.	It gives recommendations for safeguarding personal data stored in the cloud (Personally Identifiable Information - PII) and facilitates organizations in showcasing their adherence to data protection rules.	European Cybersecurity Certification Scheme for Cloud Services concentrates on the specific functionalities provided by a cloud service to its customers, based on the resources used.

Table 1. Comparison of certification framework: Key elements

These dynamics around cloud certification and regulatory fragmentation are particularly relevant for research and innovation projects like SMAUG, which rely on robust digital infrastructures to manage sensitive data across borders. To operationalize EU-wide standards in practice, especially within critical domains such as maritime surveillance, it is essential to align cybersecurity certification efforts with data governance strategies.

Consistency Implications and Recommendations

To enhance data governance in maritime security projects, under the SMAUG WP2 some key recommendations regarding datasets have been developed, including, for example:

- If the data structure is unclear, it will be necessary to engage with data sources to clarify expected structured data output;
- If there is a poor generalization ability of ML models, it will be necessary to request additional real world data from partners;
- In case there is no time for testing AI Decision Making in real world scenarios, it may be useful to create a virtual scenario – like a digital twin - to train and test the AI model.

A further critical element in policy development is ensuring that cybersecurity measures align with EU regulatory frameworks such as the Cyber Resilience Act. As AI systems become more integrated into maritime surveillance, policymakers must also define clear liability mechanisms for AI-based decision-making. Ensuring accountability and compliance with international maritime laws will be crucial in the coming years. The digital transformation of maritime security requires a comprehensive data governance strategy that balances innovation, security, and regulatory compliance. The SMAUG project exemplifies how AI-driven technologies can enhance threat detection while adhering to EU data governance policies. Future research should explore the intersection of AI ethics, cybersecurity, and international maritime law to further refine data governance strategies in the maritime domain. Policymakers must continue to refine regulatory frameworks that ensure AI's responsible use in surveillance operations while maintaining high standards of data protection and privacy.

In this regard, it is useful to consider a recent Center for Information and Policy Leadership Report (*Privacy-Enhancing and Privacy- Preserving Technologies in AI: Enabling Data Use and Operationalizing Privacy by Design and Default*)[18]which explores privacy-enhancing technologies (PETs and PPTs) in the context of AI, highlighting their role in ensuring data privacy and security during the development and deployment of AI systems, in a perspective which seems to be really meaningful and promising in SMAUG project.

Trying to summarize the content of the report[19], we may remind that Privacy-Enhancing Technologies (PETs) and Privacy-Preserving Technologies (PPTs) offer significant promise. These

[18] cipl_pets_and_ppts_in_ai_mar25.pdf .

[19] Already In December 2023, the CIPL published a white paper titled *"Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age."* This foundational document provided a comprehensive overview of PETs, real-world case studies, and practical insights into their implementation. It also identified key barriers to adoption and outlined strategies for overcoming them. Among its most important recommendations were:

- Provide Regulatory Clarity and Incentives: Governments and regulatory bodies should issue clear guidance on the legal use of PETs and offer incentives for adoption. Legal certainty is essential for organizations to confidently invest in and deploy PETs. Safe harbors, liability mitigations, and alignment with regulatory concepts (e.g., anonymization under data protection laws) can encourage responsible adoption and innovation.
- Promote Education and Awareness: A lack of understanding among stakeholders—businesses, developers, and individuals—remains a major barrier. PET providers should demonstrate the tangible value of these technologies, especially through concrete case studies. Organizations must also understand PET limitations and how to apply them contextually. Public education will build trust and strengthen digital confidence.

technologies provide innovative ways to protect privacy and ensure cybersecurity, while still enabling data sharing and reuse across different entities, sectors, and borders. In doing so, PETs serve as vital enablers of business, facilitating responsible AI development and deployment in a way that respects both privacy rights and commercial interests. By design, PETs support not only privacy but also the protection of confidential and proprietary information, thus helping organizations meet legal obligations and uphold data protection principles. Their role becomes even more critical as AI adoption accelerates and the demand for secure, ethical, and trustworthy data practices intensifies. International organizations such as the OECD have recognized the importance of PETs and are actively contributing to ongoing efforts in this space.

The PETs family includes a broad range of technical solutions that can be applied at various stages of the AI lifecycle. For example, federated learning allows machine learning models to be trained on decentralized data without transferring that data to a central location, reducing the risk of privacy breaches. Homomorphic encryption enables secure computation on encrypted data, even across borders, making it possible for multiple parties to train models collaboratively without ever exposing their raw data. Other techniques like differential privacy and synthetic data generation help to anonymize or de-identify datasets used in AI development.

These technologies collectively make it possible to operationalize privacy by design and by default—principles that are foundational to modern data protection laws. However, it's important to acknowledge that PETs are not a cure-all. They may not be suitable for every scenario, and trade-offs between data utility and privacy protection often remain. Rather than being viewed as standalone solutions, PETs should be considered part of a broader toolkit for responsible AI and data governance in SMAUG project.

Different PETs are optimized for different stages of the AI development process, from data collection and training to deployment and monitoring. Probably, the most effective privacy-preserving

---

- Develop Industry Standards: The absence of universally accepted standards for many PETs limits interoperability and scalability. While standards exist for certain techniques (e.g., homomorphic encryption), others like differential privacy are still maturing. Establishing technical standards and frameworks would enhance consistency, foster cross-jurisdictional compatibility, and increase trust in PET implementations.

Recognize PETs as Accountability Tools: PETs should be viewed as key components of accountable data governance. They align well with frameworks such as CIPL's own Accountability Framework, and help demonstrate an organization's commitment to minimizing risk, protecting individuals, and enabling innovation through responsible data stewardship. The White paper can be read here: cipl-understanding-pets-and-ppts-dec2023.pdf

strategies involve combining multiple PETs to achieve the desired balance between data usability and protection.

Looking ahead, a complementary area requiring attention is cloud services certification, which plays a critical role in supporting secure data infrastructures and enabling compliant AI deployment. As maritime security projects like SMAUG increasingly rely on cloud-based solutions for data processing and sharing, there is a pressing need to ensure these platforms meet consistent and robust regulatory standards across the EU.

To address this, we propose the development of an "EU Cloud Governance Manual", offering a comprehensive reference for cloud-related legal and regulatory guidelines in Europe. This initiative would:

- Compile both mandatory and non-mandatory rules into an accessible format;
- Provide a user-friendly, interactive website for both providers and users;
- Establish a periodic review process involving EU and national authorities;
- Create a voluntary compliance registry for cloud service providers.

Such a manual would significantly enhance transparency, legal certainty and harmonization across the EU, supporting secure and compliant cloud deployment for all stakeholders. Ultimately, it would help align emerging technologies, such as AI in maritime security, with a consistent and forward-thinking regulatory ecosystem.