GIS Odyssey Journal

2026 • Volume 6 • Number 1

https://doi.org/10.57599/gisoj.2026.6.1.213

Maciej Kiedrowicz[1], Kazimierz Worwa[2]

MODELING THE SECURITY AND RESILIENCE OF GIS SYSTEMS USING ARTIFICIAL INTELLIGENCE

Abstract: Geographic information systems (GIS) play a critical role in the functioning of modern states and economies by supporting crisis management, critical infrastructure protection, and the delivery of public services. The increasing integration of GIS with cloud computing environments, Internet of Things (IoT) networks, and real-time analytical mechanisms significantly enhances their operational capabilities, but at the same time increases system complexity and exposure to cyber threats, technical failures, and operational disturbances. This paper proposes an integrated approach to modeling the security and resilience of GIS systems using artificial intelligence techniques, including machine learning, neural networks, and probabilistic modeling. The proposed framework supports automated anomaly detection, vulnerability forecasting, and assessment of the impact of disruptions on the operational continuity of geoinformatics components across data, analytical, and service layers. The model explicitly accounts for data quality, AI model stability, and API-based service behavior within a unified resilience assessment structure. Experimental results demonstrate that AI-based solutions enable earlier identification of incidents and more effective analysis of GIS resilience compared to conventional methods. In particular, the proposed approach improves detection of subtle anomalies and supports systematic evaluation of cascading effects under compound disturbance scenarios. The findings confirm the potential of artificial intelligence to enhance the automation and adaptability of GIS security processes and provide a foundation for further research on intelligent, adaptive mechanisms for spatial data protection and resilient geoinformatics infrastructures.

Keywords: GIS systems, spatial information security, the resilience of systems, artificial intelligence, risk modelling

Received: 15 April 2026; accepted: 7 June 2026; revised: 11 June 2026

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

[2] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-8153-958X, email: kazimierz.worwa@wat.edu.pl

Introduction with analysis of the state of the problem

The rapid development of information and communication technologies, combined with the growing availability of spatial and spatio-temporal data, has made geographic information systems (GIS) a fundamental component of public administration, economic activity, and critical infrastructure management. Contemporary GIS platforms increasingly operate in distributed and cloud-based environments, process data in near real time, and integrate information from heterogeneous sources such as IoT devices, GNSS sensors, and web services. While these capabilities significantly enhance analytical power and decision-support functions, they simultaneously increase system complexity and expand the attack surface exposed to cyber threats.

Recent studies indicate that vulnerabilities related to the manipulation of positioning signals and attacks targeting service layers constitute one of the fastest-growing threat vectors for modern geoinformatics systems (Meng et al., 2022). The consequences of such incidents extend beyond technical malfunctions and may include disruption of decision-making processes, loss of spatial data integrity, erosion of trust in analytical outputs, and interruptions in critical spatial services supporting transportation, emergency response, and infrastructure monitoring (Goodchild, 2012). As GIS systems increasingly support safety-critical and mission-critical operations, ensuring their security and resilience becomes a priority rather than a secondary technical concern.

The growing complexity and sophistication of contemporary threats have revealed the limitations of traditional, rule-based protection mechanisms. As a result, there is an increasing interest in the application of artificial intelligence (AI) methods for enhancing the detection and mitigation of anomalies in GIS environments. Recent research demonstrates that machine learning and deep learning approaches, including neural networks and generative models, can significantly improve the detection of subtle GNSS signal manipulations, particularly in scenarios where classical signal-processing techniques fail (Chen et al., 2025). The ability of AI models to jointly analyze temporal, spatial, and statistical features enables the identification of hidden and gradually evolving anomalies, making AI a promising instrument for the protection of spatial data and geospatial services.

At the same time, studies on the application of AI in the cybersecurity of location-based systems confirm that deep learning methods are capable not only of classifying different types of interference, but also of distinguishing between legitimate signal disturbances and malicious manipulations with effectiveness exceeding that of traditional approaches (Ghanbarzade & Soleimani, 2025). These results highlight the necessity of developing broader analytical frameworks that integrate data quality assessment, GIS system architecture, and advanced anomaly detection mechanisms into a unified model (Devillers et al., 2007; ISO, 2023; Psiaki & Humphreys, 2016; Humphreys, 2012; RTCA, 2016).

Despite intensive research efforts, the literature still lacks a coherent and methodologically consistent framework that enables a comprehensive assessment of the role of artificial intelligence in protecting geospatial data and services. In particular, the

integration of formal spatial data quality measures, AI model stability, and service-layer cybersecurity within a single analytical construct remains insufficiently addressed. Existing studies tend to focus on isolated components, such as data accuracy, anomaly detection algorithms, or network security, without considering their interdependencies within complex GIS architectures.

In response to this gap, the present study formulates four research questions:

1) how artificial intelligence methods can be effectively used for identifying threats in GIS systems,
2) how the effectiveness of spatial data and signal anomaly detection techniques can be systematically analyzed,
3) how the integration of AI-based solutions into GIS infrastructures influences the assessment of system resilience, and
4) hat limitations and challenges arise from the use of AI in geospatial data security (Hollnagel, 2011; Linkov & Trump, 2019; National Academies of Sciences, 2018; Vasdev, 2020).

The primary objective of this article is to develop and demonstrate an integrated model that combines artificial intelligence techniques with data protection mechanisms and GIS services, enabling resilience assessment of geoinformatics systems under controlled research conditions. The study focuses on identifying both the potential and the limitations of such solutions, as well as outlining directions for their further development, thereby providing a foundation for adaptive and intelligent methods of spatial data protection.

The contribution and novelty of the proposed approach are threefold. First, the article introduces a consistent three-layer model for assessing GIS resilience, explicitly distinguishing between data, analytical models, and API-based service layers. Second, it aligns formal spatial data quality metrics defined in ISO 19157-1 with performance indicators of AI models, enabling joint analysis of data quality and analytical robustness. Third, it proposes the GIS Resilience (Immunity) Index, integrating Data Quality Index (DQI), Model Layer Robustness (MLR), and API Resilience (API-R), together with a sensitivity validation procedure. These elements extend existing research and offer direct applicability in the design and evaluation of secure and resilient GIS infrastructures. Research on the security and resilience of GIS systems using artificial intelligence methods continues to evolve alongside the increasing complexity of geoinformatics infrastructures, the proliferation of API-based services, and the widespread adoption of cloud computing. Interdisciplinary literature addressing spatial data quality, spatio-temporal modeling, anomaly detection, and cybersecurity has expanded considerably, with recent reviews consistently identifying AI as a key enabler of automation and resilience in digital spatial infrastructures (Devillers et al., 2007; ISO, 2023).

Graph-based deep learning approaches represent a particularly promising research direction. A systematic review by Ares-Robledo et al. (2026) demonstrates the effectiveness of graph neural networks (GNNs) in detecting anomalies in networked systems by modeling dynamic structural and temporal relationships. Similarly,

Malarkkan et al. (2025) propose a causal learning framework in which anomalies in cyber-physical systems are identified through changes in causal network structures, an approach well suited to GIS infrastructures processing complex spatio-temporal data. Together, graph-based and causal models define emerging directions in resilience research for spatial data processing systems (Moriano et al., 2025; Kołodziej & Mazur, 2018).

Spatial data quality remains a critical benchmark in this context. Standards such as ISO 19157 emphasize completeness, logical consistency, and temporal accuracy as key prerequisites for reliable spatial analysis. The literature consistently reports that AI models are particularly sensitive to input data degradation, especially when dealing with large, heterogeneous datasets integrated in cloud environments (Devillers et al., 2007; Haque & Rahman, 2022; Shah & Dubaria, 2021; ISO, 2023).

Moreover, the growing reliance on web services and APIs in GIS architectures has shifted research attention toward the cybersecurity of service layers. Reviews such as that by Ji et al. (2024) demonstrate that AI-based anomaly detection methods can effectively analyze encrypted traffic by leveraging statistical and behavioural characteristics, compensating for the limitations of deep packet inspection. Similar conclusions are reported by Goswami (2024), who emphasizes the importance of AI-driven real-time monitoring in environments vulnerable to network and application-layer attacks.

Finally, research on GNSS threats and signal spoofing reveals a clear trend toward AI-based approaches capable of detecting subtle signal manipulations through phase analysis, data fusion, and spatio-temporal modeling. These methods significantly enhance detection capabilities in environments where GIS relies on positioning data and classical approaches are insufficient (Psiaki & Humphreys, 2016; Humphreys, 2012; Meng et al., 2022; Chen et al., 2025).

A synthesis of the reviewed literature highlights four key research gaps:

1) the lack of integration between formal geospatial data quality measures and AI algorithms,
2) insufficient analysis of AI model resilience to geolocation manipulation scenarios,
3) the absence of a unified approach simultaneously addressing data, analytical models, and API-based service layers; and
4) the lack of a comprehensive GIS resilience model integrating data quality, AI stability, and service security (Devillers et al., 2007; ISO, 2023).

These gaps constitute the starting point for the approach proposed in this article, which models GIS security and resilience through a layered framework combining data, models, and services.

Materials and methods

The methodological framework was developed to enable a rigorous, standards-compliant, and reproducible assessment of the security and resilience of contemporary geographic information systems supported by artificial intelligence. In accordance with the research objectives and the problem analysis presented in the introductory section,

the methodology integrates spatial data quality assessment, AI-based anomaly detection, and service-layer security evaluation within a unified experimental model. The adopted approach reflects the architectural complexity of modern GIS platforms operating in distributed, cloud-based, and API-oriented environments and addresses the need for coherent analysis across data, analytical models, and service interfaces.

The methodology is based on the assumption that GIS resilience is an emergent system property resulting from interactions between three interdependent layers: spatial data, artificial intelligence models, and service infrastructure. At the data layer, spatial data quality is formalized in accordance with ISO 19157-1:2023 and treated as a measurable and controllable factor influencing downstream analytical performance. At the analytical layer, artificial intelligence methods are used to detect anomalies and disturbances that cannot be reliably identified using deterministic rules or static thresholds, particularly in spatio-temporal and signal-based contexts. At the service layer, GIS functionality is delivered via standardized OGC API–Features interfaces, whose exposure to application-level threats requires resilience assessment based on observed operational behavior rather than perimeter-based security mechanisms.

To support controlled experimentation, three categories of datasets were prepared: spatial vector data, simulated GNSS signal data, and GIS service telemetry. The spatial dataset represents a synthetic, yet structurally realistic urban environment composed of point and linear features linked by explicitly defined topological relationships. A complete set of metadata compliant with ISO 19157-1:2023 accompanies the dataset, enabling formal modeling of data quality degradation. Controlled modifications were introduced incrementally, including reductions in completeness, introduction of logical and topological inconsistencies, temporal delays, and thematic inaccuracies. This procedure preserves semantic realism while ensuring traceability between data quality degradation and observed analytical effects.

GNSS signal data were generated using simulated urban trajectories designed to reflect typical navigation conditions in dense built environments. Both nominal signals and intentionally manipulated signals were included, covering gradual displacement scenarios, phase and timing perturbations, and abrupt positional shifts documented in the literature. Simulation parameters such as sampling frequency, route length, travel time, and noise characteristics were selected to approximate real-world operational conditions. This design enables systematic assessment of AI models under a wide spectrum of signal disturbances, ranging from subtle anomalies to severe manipulations.

Service-layer data were obtained from an implementation compliant with the OGC API–Features specification. System behavior was monitored under nominal operation, overload conditions, and adversarial scenarios aligned with the OWASP API Security Top 10 classification. Telemetry included request volumes, response latencies, error rates, and call structure characteristics. This setup supports resilience analysis based on observable service behavior, which is particularly relevant in encrypted and distributed environments where content-based inspection is limited.

Spatial data quality assessment strictly followed the ISO 19157-1:2023 framework, covering completeness, logical and topological consistency, thematic accuracy, temporal

accuracy, and fitness for use. Each quality element was subjected to controlled degradation within predefined ranges and expressed as normalized quality indicators. These indicators were subsequently used as explanatory variables in the evaluation of AI model behavior, allowing analysis of both individual and cumulative effects of data degradation.

Artificial intelligence models were selected to reflect the heterogeneous nature of GIS data and threat vectors. Graph neural networks were applied to capture structural dependencies and topological changes in spatial datasets. Recurrent neural network and long short-term memory architectures were used to analyze GNSS time series and detect temporal anomalies. Service-layer behavior was evaluated using deep autoencoder models trained on traffic and telemetry features, enabling anomaly detection without access to packet payloads. All models were trained and evaluated under nominal conditions as well as under progressively disturbed scenarios affecting different system layers.

Experimental scenarios were designed to represent increasing system stress and complexity. Spatial data scenarios involved progressive degradation of quality attributes, GNSS scenarios varied the intensity and dynamics of signal manipulation, and service-layer scenarios combined targeted API-level attacks with high traffic loads approaching operational capacity limits. This experimental design supports analysis of GIS resilience as a gradual and multidimensional degradation process rather than a binary outcome.

Evaluation metrics were aligned with the three-layer system model. Model-level performance was assessed using standard anomaly detection measures, including precision–recall AUC, F1 score, false positive rates, and time to detection, with particular emphasis on the stability of decision thresholds under degraded input conditions. Service-layer performance was evaluated using availability, response latency, error behavior, and compliance with API operational thresholds. These metrics provide the empirical basis for integrative resilience assessment.

To enable a synthetic and comparable evaluation across scenarios, a composite GIS Resilience Index was defined. The index integrates indicators derived from data quality assessment, AI model robustness, and service-layer stability into a normalized measure expressing the overall capability of the system to maintain operational integrity under adverse conditions.

Formally, the GIS Resilience Index $\mathcal{R}_{GIS} \in [0,1]$is defined as a weighted combination of three components:

$$\mathcal{R}_{GIS} = \alpha \cdot DQI + \beta \cdot MLR + \gamma \cdot API\text{-}R$$

where:

- DQIdenotes the Data Quality Index derived from ISO 19157-1 quality elements,
- MLR represents the resilience of AI models expressed through normalized performance and stability metrics,
- and $API\text{-}R$ describes service-layer resilience based on availability, latency, and security indicators.

The weighting coefficients α, β, and $\gamma$are non-negative and satisfy $\alpha + \beta + \gamma = 1$, allowing scenario-dependent prioritization of data integrity, analytical robustness, or

service continuity. The formal construction of the index ensures transparency, reproducibility, and direct applicability in experimental evaluation.

Results and discussion

The experimental evaluation was conducted in accordance with the layered methodological framework presented earlier and covered the complete functional scope of the investigated GIS system. The results encompass spatial data quality and its influence on AI-based anomaly detection, the robustness of artificial intelligence models to GNSS signal manipulation, and the stability and security of GIS services exposed through OGC API–Features. A structured overview of assessment areas, metrics, and normative references is provided in Table 1, which constitutes the analytical backbone for the interpretation of the results presented in this section.

Table 1. Areas of analysis and a set of assessment indicators used

Area of analysis	Purpose of the assessment	Indicators used	Normative basis / sources
1. Data quality	Assess the quality of input data and its impact on the performance of AI models	completeness; coherence; thematic accuracy; temporal accuracy	ISO 19157-1:2023
2. SI models	Evaluation of the effectiveness and resilience of models, including GNSS manipulation	AUC-PR; F1; FPR@k; TTD (time-to-detect)	Scientific literature, good industry practices
3. API Services	Evaluation of reliability, stability, and security of services	latency; availability; 5xx errors; compliance with OGC API – Features / ISO 19168-1; OWASP API Security Top 10 (2023) coverage	OGC; ISO; OWASP 2023
4. Resistance Index	Integrate three layers of metrics into a uniform synthetic indicator	Standardized metrics from three layers	ENISA ETL 2024 (ENISA., 2024)

Source: own elaboration

The analysis of spatial data quality degradation confirms that quality attributes defined in ISO 19157-1:2023 exert a direct and systematic influence on the behavior of AI

models. As illustrated in Fig. 1 and 2, controlled reductions in data completeness lead to a progressive decline in detection effectiveness.

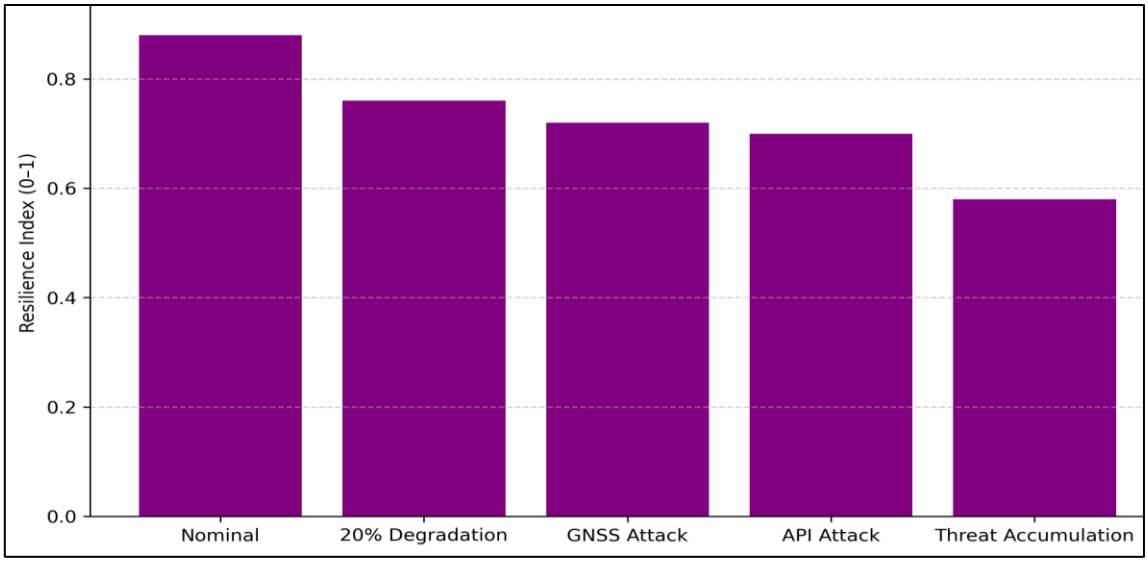

Fig. 1. Effect of data completeness on AUC-PR (synthetic data)
Source: own elaboration

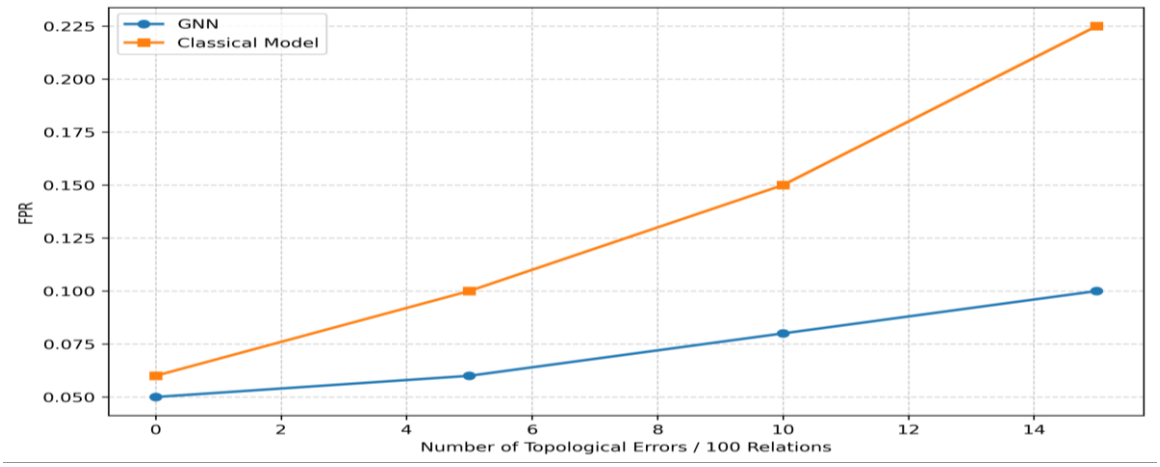

Fig. 2. The impact of data completeness on FPR (synthetic data)
Source: own elaboration

When simulated data loss exceeded approximately 20%, a clear reduction in AUC-PR was observed, accompanied by a sharp increase in false positive rates. Further degradation resulted in visible instability of decision thresholds, indicating that limited spatial coverage restricts the capacity of models to maintain consistent anomaly discrimination. These results demonstrate that even moderate data incompleteness propagates non-linearly through the analytical pipeline and significantly impacts operational reliability.

Topological consistency was identified as a particularly critical quality dimension. Experiments introducing between 5 and 15 topological errors per 100 spatial relations revealed marked differences between classical detection models and topology-aware

graph neural networks. As shown in Fig. 3 and 4 (Ares-Robledo, Rifà-Pous, & Clariso, 2026).

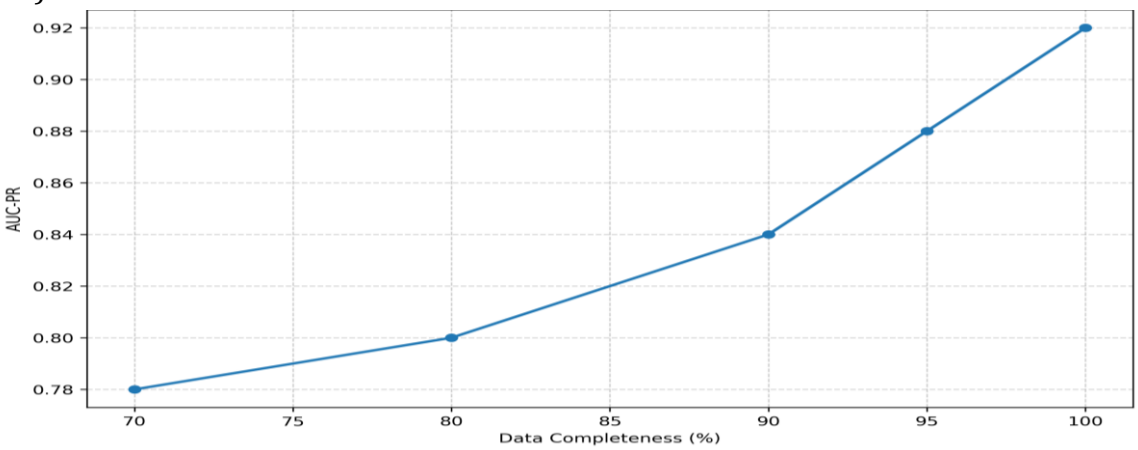

Fig. 3. The effect of topological errors on AUC-PR (GNN vs. classical model)
Source: own elaboration

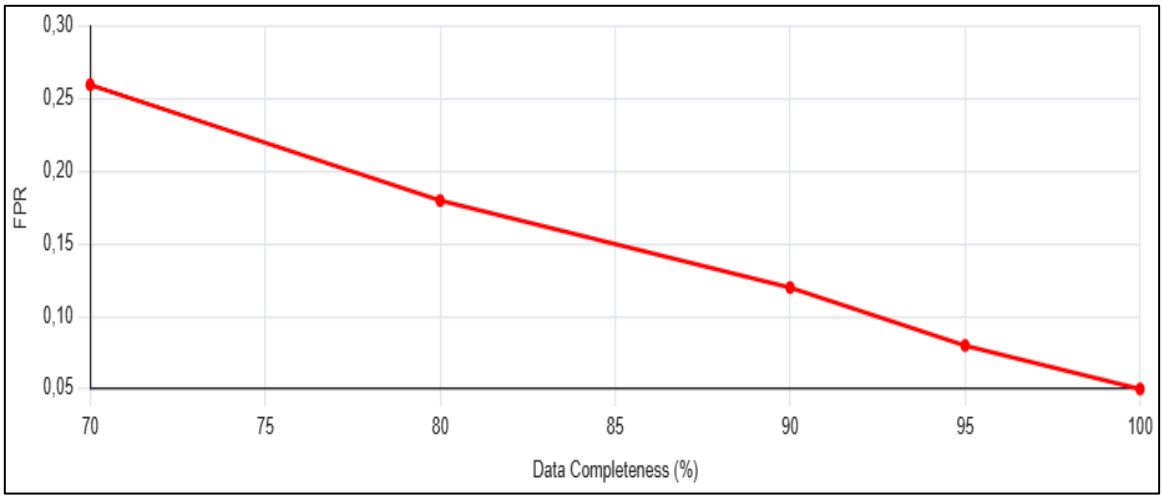

Fig. 4. The impact of topological errors on FPR
Source: own elaboration

GNN-based models exhibited substantially higher robustness, with only moderate decreases in AUC-PR and a significantly slower growth of false positives. This behavior reflects the ability of graph architectures to encode relational dependencies and maintain coherent internal representations despite localized structural inconsistencies. In contrast, non-graph models responded to the same disturbances with rapid degradation, confirming the importance of explicitly modeling spatial topology in resilient GIS analytics.

Temporal and thematic inaccuracies further influenced model behavior, particularly in multimodal analytical settings. Update delays ranging from one to several weeks and contamination of semantic attributes led to reduced detector sensitivity and increased false alarm rates. The strongest effects occurred when temporal and thematic degradations co-occurred, demonstrating cumulative semantic disruption. These findings

confirm that ISO-defined data quality dimensions – especially completeness and topological consistency – are strong predictors of AI model stability and should be treated as first-order factors in operational geoinformatics systems.

The immunity of AI models to GNSS signal manipulation was assessed using representative spoofing scenarios described in the literature, including capture-and-drag-off, phase manipulation, and abrupt phase jumps. The results demonstrate a clear advantage of AI-based approaches over classical GNSS integrity mechanisms. As illustrated in Fig. 5, sequential LSTM models and hybrid GNN+LSTM architectures achieved significantly shorter times to detection than reference methods such as RAIM and pseudo-range consistency tests.

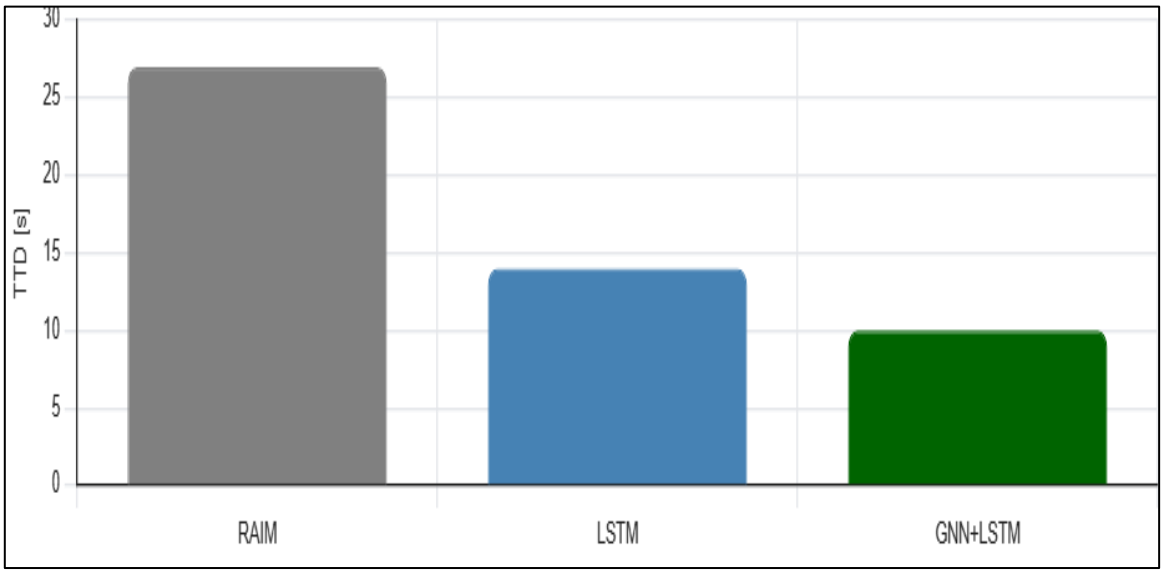

Fig. 5. Time to Detection (TTD) for GNSS Spoofing: RAIM vs. LSTM vs. GNN+LSTM
Source: own elaboration

In the majority of cases, spoofing attempts were detected within operationally relevant timeframes, often below 10 s. Slow drag-off scenarios, which represent one of the most challenging forms of GNSS manipulation, further highlighted the advantages of AI-based detection. In these experiments, traditional methods frequently interpreted gradual deviations as legitimate signal noise, whereas AI models detected subtle inconsistencies with substantially higher effectiveness. The fusion of GNSS time series with spatial context and service-layer telemetry further improved performance, confirming that multimodal representations enable the detection of cross-layer anomalies invisible to single-domain analyses.

The analysis of the service layer focused on the behavior and resilience of GIS services implemented in accordance with the OGC API–Features standard under nominal, peak, and adversarial conditions. As shown in Fig. 6, services reinforced with AI-based anomaly detection and aligned with OWASP API Security Top 10 controls exhibited significantly improved stability compared to non-AI configurations.

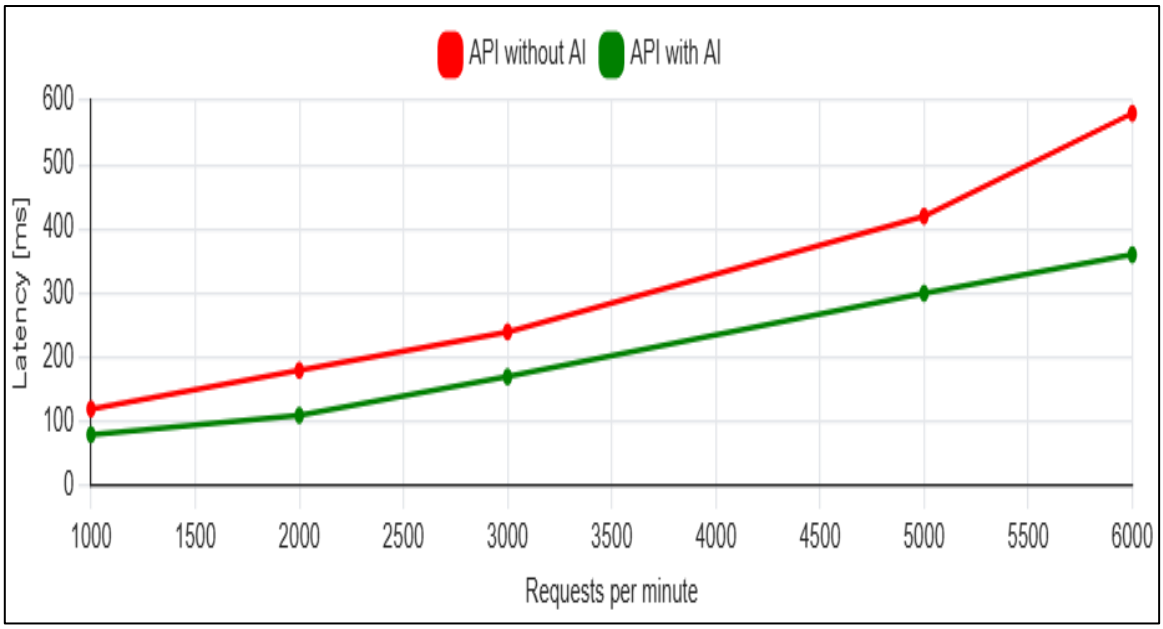

Fig. 6. API resiliency under load (latency vs number of requests/min) – comparison of non-AI and non-AI APIs
Source: own elaboration

Authorization vulnerabilities such as BOLA were consistently detected and mitigated. Under volumetric load, services without AI support experienced severe latency degradation, while AI-assisted traffic classification and rate-limiting mechanisms substantially reduced response-time growth and limited false-positive blocking. Telemetry-based monitoring also enabled detection of anomalous patterns associated with server-side request forgery and service misconfiguration, demonstrating the effectiveness of behavioural analysis in encrypted traffic environments.

To integrate the heterogeneous experimental results into a single analytical measure, the composite GIS Resilience Index was explicitly applied in the results analysis using the formal model introduced in the Methods section. The index aggregates the resilience contributions of the data, model, and service layers according to the following formulation:

$$\mathcal{R}_{GIS} = \alpha \cdot DQI + \beta \cdot MLR + \gamma \cdot API\text{-}R$$

where: $\mathcal{R}_{GIS} \in [0,1]$ denotes the overall system resilience, DQI represents the Data Quality Index derived from ISO 19157-1 quality elements, MLR expresses the robustness of AI models based on normalized performance and stability metrics, and $API\text{-}R$ quantifies service-layer resilience using availability, latency, error behavior, and security indicators. The weighting coefficients α, β, and γ satisfy $\alpha + \beta + \gamma = 1$ and allow scenario-dependent prioritization of resilience components.

In accordance with this component-based aggregation model, the computed index values for both nominal and disturbed scenarios are presented in Fig. 7.

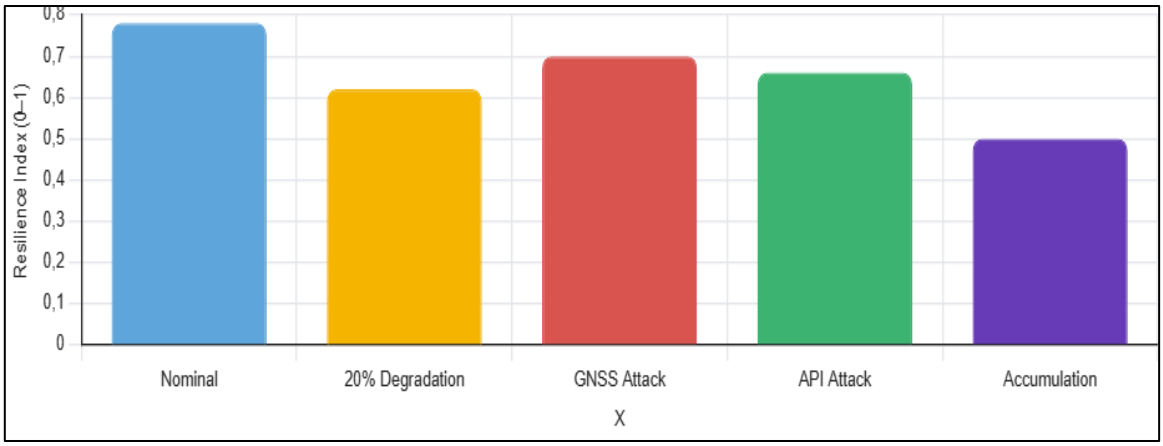

Fig. 7. Composite GIS resilience
Source: own elaboration

Under baseline conditions, the system exhibited balanced resilience, with the data quality component typically constituting the lowest contribution and the model layer the highest. Isolated disturbances resulted in moderate index reductions. However, the most pronounced resilience loss occurred in cumulative scenarios where spatial data degradation, GNSS spoofing, and API overloads co-occurred. In such cases, disturbances propagated across layers, amplifying their individual effects and leading to rapid degradation of overall system resilience. This behavior is consistent with the linear aggregation model of the index, in which simultaneous degradation of multiple components results in compounded resilience loss. A strong positive relationship between the Data Quality Index and Model Layer Robustness is illustrated in Fig. 8.

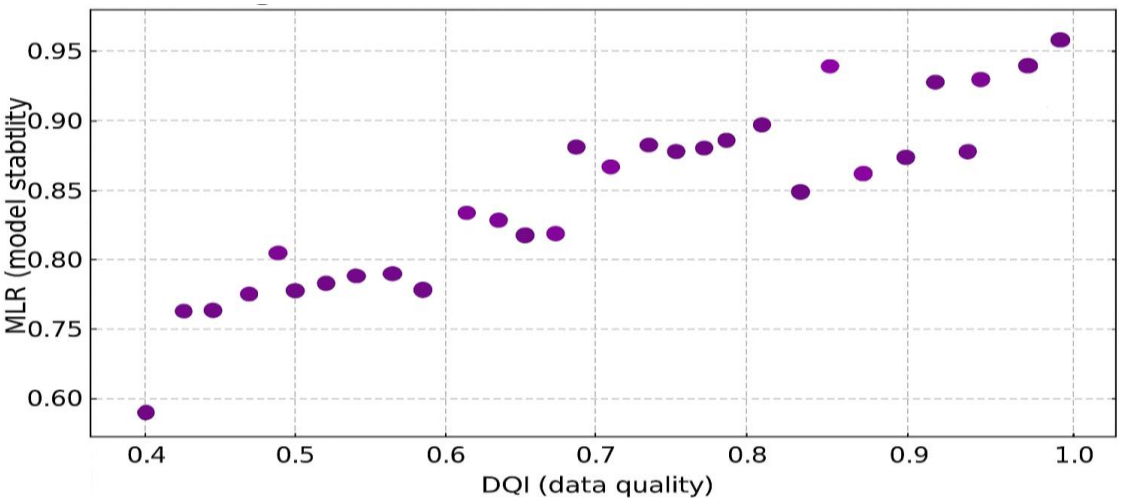

Fig. 8. DQI–MLR correlation (the lower the data quality, the lower the stability of the models)
Source: own elaboration

As DQI values declined, AI model stability decreased systematically, leading to increased false positive rates and greater threshold instability. This relationship

remained evident even for advanced architectures such as GNNs and LSTM-based models, indicating that increasing model complexity does not eliminate dependence on high-quality input data. These results underscore the fundamental role of data quality in sustaining reliable AI performance in GIS environments.

From a broader perspective, the results align with current trends in GeoAI and the increasing autonomy of geoinformation systems (Janowicz et al, 2020; Li & Hsu, 2023; Yuan & Wang, 2020). As AI models assume a growing share of analytical and decision-support functions, system resilience becomes contingent upon coordinated management of data quality, model robustness, and service security. The experiments confirm that AI can effectively compensate for limitations of classical monitoring techniques—particularly in encrypted traffic analysis and spatio-temporal anomaly detection—but only when embedded within a coherent, standards-compliant, multi-layered framework.

The practical implications of these findings are significant for GIS deployments in public administration, crisis management, and critical infrastructure. The results demonstrate that resilience cannot be achieved through isolated technical measures applied to individual layers. Instead, sustained resilience requires formal data quality governance compliant with ISO 19157-1, secure and observable service architectures aligned with OGC and OWASP standards, and adaptive AI-based anomaly detection operating across layers. The proposed GIS Resilience Index provides a transparent and extensible instrument for integrating these dimensions and identifying operational thresholds at which cumulative disturbances pose a risk to system continuity.

In summary, the results and their integrated interpretation confirm that the security and resilience of GIS systems are inherently multi-dimensional and interdependent. Spatial data quality, AI model behavior, and service-layer stability jointly determine the ability of GIS infrastructures to withstand, absorb, and adapt to adverse conditions. The presented framework and explicitly applied resilience model establish a robust foundation for further research into adaptive, explainable, and autonomous security mechanisms for geospatial information systems.

Case Study. The purpose of this case study is to empirically verify the proposed approach to modeling the security and resilience of geographic information systems using artificial intelligence methods in a homogeneous and controlled research environment that reflects typical operating conditions of urban geoinformatics infrastructure. The case study is analytical rather than implementation-oriented and is designed to enable reproducible assessment of system behavior under disturbances simultaneously affecting the data layer, analytical models, and service layer. The analyzed environment represents a hypothetical yet operationally realistic GIS supporting a metropolitan area of approximately 450 km^2, corresponding to the structure of systems deployed in large urban agglomerations. The spatial dataset consists of 12,800 linear features, including road and tram networks, and 1,150 point features representing elements of critical infrastructure such as power substations, fire stations, and hospitals. In addition, 320 explicitly defined topological relationships describing connectivity and adjacency were included. The data were stored in GeoJSON and GeoPackage formats and accompanied by

a complete set of ISO 19157-1:2023–compliant data quality metadata, enabling formal and unambiguous modeling of data quality degradation.

Spatial data quality assessment and degradation scenarios were designed in accordance with ISO 19157-1:2023. Completeness, logical and topological consistency, thematic accuracy, and temporal accuracy were treated as key quality dimensions influencing the stability of analytical processes. Quality indicators served simultaneously as diagnostic variables and as input features for AI models. Controlled degradation included progressive data loss (5–30%), introduction of logical and topological inconsistencies (5–15 errors per 100 relationships), extension of data update latency from below 48 h to 7–30 days, and intentional distortion of 3–12% of thematic attribute values. These scenarios correspond to typical data quality issues observed in operational GIS environments.

GNSS data used in the case study were generated through simulation of urban travel trajectories with a sampling frequency of 1 Hz, an average route length of 35 km, and a travel duration of approximately 52 min. Natural measurement noise with an amplitude of ± 1.5 m was incorporated to preserve realism. Three classes of signal manipulation scenarios were implemented: gradual signal takeover and displacement (*capture and drag-off*), phase and timing manipulations affecting pseudorange estimation, and abrupt phase jumps resulting in instantaneous position shifts. These scenarios are widely recognized as particularly difficult to detect using classical GNSS integrity monitoring mechanisms.

The service layer was implemented using an interface compliant with the OGC API–Features specification (ISO 19168-1), providing access to collections and features with support for spatial queries. Services were fully instrumented for telemetry, capturing response latency, error behavior, and traffic characteristics. Under nominal conditions, the system processed approximately 530 requests per minute, while stress scenarios included peak loads of 1,800–2,300 requests per minute and volumetric attack simulations reaching 4,500–6,000 requests per minute, corresponding to levels observed in contemporary large-scale DDoS campaigns. Security evaluation was conducted with reference to the OWASP API Security Top 10 classification, focusing on object-level authorization flaws (BOLA), unlimited resource consumption, server-side request forgery (SSRF), and service misconfigurations.

Three classes of artificial intelligence models were applied in the case study in line with the characteristics of the analyzed data. Graph neural networks were used to analyze spatial relationships and topological structures, sequential LSTM/RNN models were employed to detect subtle GNSS signal manipulations, and a deep autoencoder was applied to the analysis of encrypted API traffic without performing deep packet inspection. Model configurations and acceptance criteria were consistent with those used in the experimental evaluation, ensuring methodological continuity and comparability of results.

System resilience assessment was integrated using the composite GIS Resilience Index, explicitly applied to the case study scenario. The index was computed according to the following relationship:

$$\mathcal{R}_{GIS}^{(CS)} = \alpha \cdot DQI^{(CS)} + \beta \cdot MLR^{(CS)} + \gamma \cdot API\text{-}R^{(CS)}$$

where: $\mathcal{R}_{GIS}^{(CS)}$ denotes the resilience level of the GIS in the analyzed case study, calculated in accordance with the formal definition of the GIS Resilience Index presented in the *Materials and Methods* section, and the superscript (CS) indicates values specific to this application scenario. Equal component weights ($\alpha = \beta = \gamma$) were adopted, reflecting the assumed equal importance of data quality, analytical robustness, and service continuity in typical urban GIS deployments.

Application of the index enabled clear differentiation between nominal system operation, isolated degradation scenarios, and cumulative scenarios in which data quality degradation, GNSS manipulation, and service overload occurred simultaneously. Consistent with the additive structure of the model, cumulative scenarios resulted in disproportionately large resilience loss, confirming the propagation and mutual amplification of disturbances across system layers.

As illustrated in Fig. 9, a disproportionately large decline in system resilience is observed when disturbances simultaneously affect the data layer, the analytical model layer, and the service layer. In contrast, isolated disturbances impacting individual layers of the GIS architecture lead only to a moderate reduction in the value of the resilience index. Cumulative disturbance scenarios, however, result in a sharp decrease in $\mathcal{R}_{GIS}$, reflecting complex interactions between spatial data quality degradation, reduced stability of AI-based analytical models, and performance limitations of the service layer. This behavior confirms the systemic nature of GIS resilience and demonstrates that concurrent multi-layer disruptions significantly amplify the adverse effects on overall system performance.

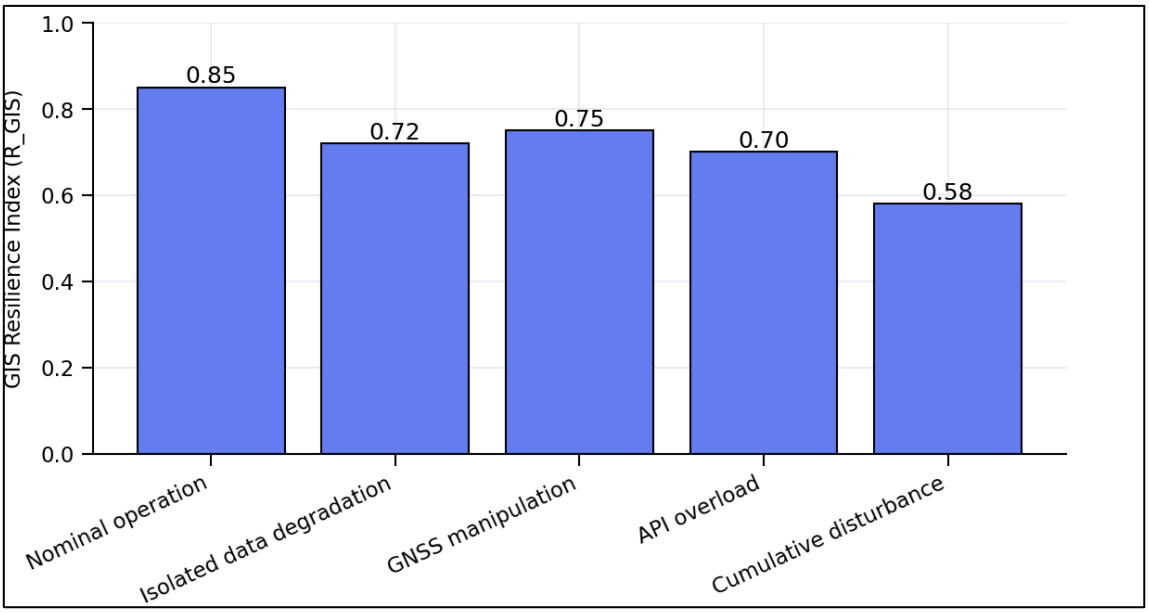

Fig. 9. Synthetic illustration of the GIS Resilience Index ($\mathcal{R}_{\mathrm{GIS}}$) for the analyzed case study under nominal conditions, isolated disturbances, and cumulative multi-layer disturbances
Source: own elaboration

The case study demonstrates that the proposed approach enables a transparent, standards-compliant, and reproducible assessment of GIS resilience in an environment closely resembling real-world conditions. Integrating formal data quality measures, AI model performance indicators, and service-layer telemetry within a single analytical construct allows coherent interpretation of system behavior under compound threat conditions. The results clearly indicate that maintaining high GIS resilience requires coordinated management of all three layers, while isolated optimization of individual components is insufficient under cumulative disturbance scenarios.

For clarity and conciseness, the numerical values of the GIS Resilience Index used in this case study are consistent with those reported in the experimental evaluation and are therefore not repeated here to avoid redundancy.

Conclusions

This study addressed the growing challenge of ensuring the security and resilience of contemporary geographic information systems operating in distributed, data-intensive, and service-oriented environments. By integrating spatial data quality assessment, artificial intelligence–based anomaly detection, and service-layer security analysis within a unified framework, the paper contributes a coherent approach to modeling GIS resilience under coordinated disturbances affecting data, analytical models, and operational services.

The results demonstrate that spatial data quality, formalized in accordance with ISO 19157-1:2023, constitutes a fundamental determinant of AI model stability and reliability. Degradation of completeness and topological consistency was shown to significantly increase false positives and destabilize decision thresholds, even when advanced architectures such as graph neural networks and recurrent models were applied. These findings confirm that improvements at the model level cannot compensate for structural deficiencies in input data and that data quality must be treated as a first-order resilience factor in GIS-AI pipelines.

The evaluation of GNSS spoofing scenarios confirms the superiority of AI-based, multimodal approaches over classical integrity monitoring mechanisms. Sequential and hybrid graph–temporal models were able to detect subtle signal manipulations, particularly in slow drag-off scenarios, within operationally relevant timeframes. The fusion of signal dynamics with spatial context and service-layer telemetry proved essential for revealing cross-layer inconsistencies that remain undetectable when individual data streams are analyzed in isolation.

The analysis of API-based GIS services highlights that compliance with interoperability standards such as OGC API–Features is a necessary but insufficient condition for operational resilience. The integration of OWASP-aligned security controls and AI-assisted anomaly detection significantly improved service stability under both authorization abuse and volumetric stress. These results underline the importance of telemetry-driven, behavior-based monitoring in modern GIS architectures, particularly in encrypted and cloud-based environments.

A key contribution of this work is the formulation and application of the composite GIS Resilience Index, which integrates data quality (DQI), model-layer robustness (MLR), and service-layer resilience (API-R) into a single, normalized indicator. The index enables transparent, quantitative comparison of resilience across nominal, degraded, and cumulative threat scenarios. Both experimental results and the illustrative case study demonstrate that resilience losses accelerate non-linearly when disturbances propagate simultaneously across multiple layers, confirming the necessity of holistic, system-level assessment rather than isolated security measures.

From a practical perspective, the proposed framework and resilience index provide actionable guidance for organizations operating GIS in public administration, crisis management, and critical infrastructure contexts. The findings indicate that sustainable resilience requires coordinated governance of data quality, continuous monitoring and adaptation of AI models, and secure, observable service architectures. The framework is designed to be extensible and reproducible, supporting integration with existing standards and operational monitoring tools.

Several limitations of the study point to directions for future research. Although the experimental environment and case study were designed to be realistic, validation in fully operational GIS deployments remains a critical next step. Further work should explore the resilience of emerging AI architectures, including transformer-based and generative models, as well as adaptive weighting strategies for the resilience index tailored to specific operational priorities. Additional research is needed to extend the framework to cloud-native and microservice-based GIS architectures, as well as to investigate continuous, real-time resilience assessment within autonomous and self-healing geoinformation systems.

In conclusion, this study demonstrates that GIS security and resilience are inherently multi-dimensional properties arising from the interaction of data, models, and services. The proposed framework and GIS Resilience Index offer a rigorous and practically applicable foundation for analyzing these interactions and for advancing the development of resilient, intelligent, and trustworthy geospatial information systems.

Funding

This work was financed/co-financed by Military University of Technology under research project UGB 531-000091-W500-22.

Declaration of Competing Interests

Authors don't have any financial, personal, or professional relationships that could be perceived to influence the reported research.

Data Availability

No public, restricted and proprietary data collected or analyzed.

Use of Generative AI and AI-Assisted Technologies

This statement must be aligned with the journal policy and with the authors' actual use of AI and AI-assisted technologies.

References

Ares-Robledo F., Rifà-Pous H., Clariso R. (2026). Graph neural networks for anomaly detection: A systematic review of dynamic temporal approaches. Artificial Intelligence Review, 58, 1–45.

Chen L., Ouyang X., Zeng F., Rui Z., Ming Y. (2025). GNSS spoofing detection based on lightweight features and CGAN-ANN in unknown scenarios. GPS Solutions, 29, 175. https://doi.org/10.1007/s10291-025-01938-1.

Devillers R., Bédard Y., Jeansoulin R., Moulin B. (2007). Towards spatial data quality information analysis tools for experts assessing the fitness for use of spatial data. International Journal of Geographical Information Science, 21(3), 261–282. https://doi.org/10.1080/13658810600911879.

ENISA (2024). European Union Agency for Cybersecurity. ENISA Threat Landscape 2024.

Ghanbarzade A., Soleimani H. (2025). GNSS/GPS spoofing and jamming identification using machine learning and deep learning. arXiv:2501.02352. https://arxiv.org/abs/2501.02352 [access: 20.03.2026].

Goodchild M.F. (2012). The future of digital earth. Annals of GIS, 18(2), 93–98. https://doi.org/10.1080/19475683.2012.668561.

Goswami M.J. (2024). AI-based anomaly detection for real-time cybersecurity. Cybersecurity Systems, 6(2), 1–15.

Haque M., Rahman M. (2022). Security challenges in cloud-native architectures: A survey on microservices, containers, and orchestration. Journal of Network and Computer Applications, 203, 103–362.

Hollnagel E. (2011). Resilience engineering in practice. CRC Press.

Humphreys T.E. (2012). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Journal of Navigation, 65(1), 1–22.

ISO (2020). ISO 19168-1:2020. https://www.iso.org/standard/32586.html [access: 20.03.2026].

ISO (2023). ISO 19157-1:2023. https://www.iso.org/standard/78900.html [access: 20.03.2026].

Janowicz K., Gao S., McKenzie G., Hu Y., Bhaduri B. (2020). GeoAI. International Journal of Geographical Information Science, 34(14), 2583–2594.

Ji I.H., Lee J.H., Kang M.J. Park W.J. (2024). Artificial Intelligence-Based Anomaly Detection Technology over Encrypted Traffic: A Systematic Literature Review. Sensors, 24(3), 898.

Kołodziej J., Mazur M. (2018). Cyber-physical security. Journal of Applied Security Research, 13(2), 256–276.

Li W., Hsu C. (2023). Autonomous GIS. International Journal of Geographical Information Science, 37(4), 765–790.

Linkov I., Trump B.D. (2019). The science and practice of resilience. Springer.

Malarkkan A.V., Bai H., Wang X., Kaushik A., Wang D., Fu Y. (2025). Rethinking Spatio-Temporal Anomaly Detection: A Vision for Causality-Driven Cybersecurity. arXiv:2507.08177. https://arxiv.org/abs/2507.08177 [access: 20.03.2026].

Meng L., Yang L., Yang W., Zhang L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. Remote Sensing, 14(19), 4826. https://doi.org/10.3390/rs14194826.

Moriano P., Hespeler S.C., Li M., Mahbub M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. Artificial Intelligence Review, 58, 283.

National Academies of Sciences, Engineering, and Medicine (2018). Emergency and disaster resilience. National Academies Press.

OGC (2022). OGC API – Features – Part 1: Core. https://ogcapi.ogc.org/features [access: 20.03.2026].

OWASP Foundation (2023). OWASP API Security Top 10. https://owasp.org/www-project-api-security/ [access: 20.03.2026].

Psiaki M.L., Humphreys T.E. (2016). GNSS spoofing and detection. Proceedings of the IEEE, 104(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658.

Shah A., Dubaria A. (2021). Securing microservices. IEEE Software, 38(2), 76–84.

Vasdev A. (2020). Geospatial cyber-situational awareness. Journal of Information Warfare, 19(3), 45–61.

Yuan M., Wang S. (2020). Human-centric geoAI. Annals of the American Association of Geographers, 110(8), 2257–2274.