GIS Odyssey Journal

2026 • Volume 6 • Number 1

https://doi.org/10.57599/gisoj.2026.6.1.247

Stefan Rozmus[1], Jerzy Stanik[2]

A METHODOLOGICAL FRAMEWORK FOR ASSESSING THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE CYBERSECURITY OF MODERN GIS SYSTEMS

Abstract: This paper proposes an integrated methodological framework for assessing the role of artificial intelligence in the cybersecurity of contemporary geographic information systems (GIS). The framework is structured around three interrelated dimensions: spatial data quality, the resilience of anomaly detection models to geolocation manipulation, and the security architecture of geospatial service environments. The study aims to provide a coherent, simulation-based foundation for systematically examining the relationships among these dimensions in a controlled and reproducible research setting. The framework is demonstrated using synthetic yet operationally realistic data representing an urban public transport environment. The methodological design combines: (i) formal assessment of spatial data quality in accordance with ISO 19157-1:2023 and ISO 19115-1:2014; (ii) comparative evaluation of anomaly detection models implemented in single-channel and multimodal configurations; and (iii) assessment of OGC API–based geospatial services under conventional trust-based and Zero Trust security architectures. The simulation environment includes controlled data quality degradation, GNSS spoofing scenarios, and selected API abuse patterns. The results indicate that the proposed framework provides a coherent basis for analysing the effects of data quality on anomaly detection, the response of multimodal AI models to geolocation manipulation. Under simulated disruption conditions, multimodal analytical configurations and Zero Trust architectures showed greater robustness than conventional approaches. The framework offers a methodological foundation for future research on AI-supported GIS cybersecurity.

Keywords: GIS cybersecurity, artificial intelligence, spatial data quality, GNSS spoofing, Zero Trust architecture, geospatial services

Received: 15 April 2026; accepted: 27 May 2026; revised: 15 June 2026

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0003-1816-927X, email: stefan.rozmus@wat.edu.pl

[2] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl

Introduction with analysis of the state of the problems

The dynamic development of information technologies and the growing availability of geospatial data make geographic information systems (GIS) a key element of modern public administration, enterprise operations, and critical infrastructure management. Modern GIS platforms increasingly operate in distributed environments, process near-real-time data streams, and integrate information from Internet of Things devices and cloud services. These capabilities significantly expand analytical and decision-making potential, but at the same time increase the attack surface and expose GIS to complex cyber threats.

The most serious threats to GIS environments include manipulation of sensor data, GNSS spoofing, distributed denial-of-service attacks on maps and geospatial services, and unauthorised interference with spatial databases. Their effects include disruption of decision-making processes, loss of data integrity and reliability, degradation of service availability, and, in critical infrastructure contexts, the possibility of cascading failures in dependent systems. The increasing complexity, heterogeneity, and variability of threats make traditional rule-based and perimeter-oriented protection mechanisms insufficient.

In response to these challenges, artificial intelligence is becoming an increasingly important component of GIS cyber resilience. Machine learning, deep learning, and anomaly detection can help identify subtle and non-obvious patterns indicating potential security breaches or data manipulation. A major advantage of AI-based approaches is the ability to analyse spatial, temporal, and topological aspects of geospatial data simultaneously, which makes them particularly well suited to the multidimensional nature of GIS systems (Chandola et al., 2009; Goodchild, 2010).

Despite the growing number of publications on AI applications in cybersecurity, research directly related to GIS environments remains fragmented. Existing approaches typically focus on selected aspects such as anomaly detection in spatial data, GNSS spoofing detection, or network and application protection, but rarely provide a coherent framework integrating data quality, model resilience, and service-layer security architecture. In particular, systemic relationships among these three areas remain insufficiently recognised.

Fundamental work in GIScience indicates that data completeness, positional accuracy, logical consistency, and properly defined metadata are necessary conditions for reliable spatial analysis, especially in operational and critical applications (Longley et al., 2015; ISO, 2014; ISO, 2023).

These principles are directly relevant to AI-based security mechanisms because degradation or manipulation of input data can reduce model stability, increase false positives, and hinder interpretation. The anomaly detection literature further shows that unsupervised and semi-supervised methods are effective in analysing high-dimensional data but remain sensitive to distributional change and noise (Chandola et al., 2009). In GIS environments, this sensitivity is further amplified by spatiotemporal dependencies.

A substantial part of the literature concerns location data security, especially GNSS spoofing and its detection methods. These studies indicate that advanced attack strategies

may remain undetectable in traditional tracking loops unless multimodal approaches and AI methods that analyse multivariate relationships are applied (Psiaki & Humphreys, 2016; Bhatti & Humphreys, 2017; Jafarnia-Jahromi et al., 2012; Humphreys et al., 2008).

In parallel, the AI-based cybersecurity literature identifies new threat classes, such as training data poisoning and adversarial examples, which are particularly relevant in GIS systems using large and heterogeneous spatial datasets.

Scientific studies are complemented by institutional reports and technical guidelines that provide an up-to-date picture of the threat landscape. ENISA publications document the growing number of attacks targeting digital services, including geospatial platforms, with particular emphasis on breaches of availability, integrity, and continuity (ENISA, 2024). The OWASP API Security Top 10 also identifies key vulnerabilities related to authorisation, configuration, and asset management that directly affect modern GIS services exposed through APIs (OWASP Foundation, 2023).

From a normative and regulatory perspective, the functioning of secure GIS systems is shaped by multiple reference frameworks. ISO 19115-1:2014 and ISO 19157-1:2023 define formal methods for describing and evaluating spatial data quality, which can be directly integrated into AI-based analytical processes (ISO, 2014; ISO, 2023).

The OGC API – Features standard defines a modern way of publishing geospatial data in service environments, making API security a key element of GIS interoperability and resilience (OGC, 2020; OGC, 2021; OGC, 2022). At the organisational level, ISO/IEC 27001:2022 and IEC 62443 shape information security and OT/ICS protection (ISO/IEC, 2022; IEC, 2024), while in Europe the INSPIRE regulations and the NIS2 Directive are also relevant (European Parliament & Council of the European Union, 2007; European Parliament & Council of the European Union, 2022).

In the artificial intelligence domain, risk management frameworks such as NIST AI RMF 1.0 and ISO/IEC 23894:2023 are increasingly important (NIST, 2023; ISO/IEC, 2023; European Parliament & Council of the European Union, 2025).

Despite the extensive literature and normative achievements, significant research gaps remain. There is still no integrated analytical framework that simultaneously considers spatial data quality, the resilience of AI models, and the security architecture of GIS services. Three areas remain especially underdeveloped: methodological approaches combining formal quality measures with AI model stability analysis; systematic procedures for testing resilience to controlled geolocation manipulation and data degradation; and comparable frameworks for analysing GIS security architectures in both traditional and Zero Trust environments.

In response to these gaps, the article adopts three research assumptions that define the scope and structure of the proposed methodological demonstration. A1: formal measures of spatial data quality in accordance with ISO 19157-1:2023 are treated as input variables for analysing the impact of data degradation on the stability and behaviour of AI models used to detect anomalies. A2: integration of multiple information streams, such as GNSS data, quality metadata, and topological relationships, enables assessment of AI model resilience to geolocation manipulation in comparison with single-channel approaches. A3: the inclusion of Zero Trust principles, in accordance with NIST, OWASP,

and OGC good practices, enables a structured analysis of the impact of GIS service architecture on system resilience under controlled attack scenarios (NIST, 2020b; OWASP Foundation, 2023; OGC, 2020).

A comprehensive analysis of literature, standards, and reports indicates that the successful integration of AI into GIS cybersecurity requires a holistic approach based on three interrelated pillars: data quality and transparency, resilience of analytical models, and a secure and interoperable service layer. The adopted research assumptions form the basis for a demonstration case study, the purpose of which is not empirical operational validation, but the illustration of a coherent method for assessing the resilience of modern geoinformation systems.

Materials and methods

The study adopted an experimental simulation approach to assess the impact of spatial data quality, the resilience of artificial intelligence models, and service-layer security architecture on the functioning of geographic information systems under controlled conditions. The methodological framework was developed in relation to three research assumptions (A1–A3), formulated based on the current state of research and applicable standards and guidelines in the field of GIS cybersecurity.

All experiments were conducted in a dedicated simulation environment, enabling controlled modification of data quality parameters and implementation of defined attack scenarios. The research environment was designed in accordance with international standards for spatial data quality and information security (ISO, 2014; ISO, 2023; ISO/IEC, 2022). In particular, the description and assessment of data quality were based on ISO 19115-1:2014 and ISO 19157-1:2023, the publication of geospatial services followed the OGC API – Features standard, while the security architecture and threat scenarios were developed on the basis of NIST SP 800-53 Rev. 5, NIST SP 800-207, and the recommendations of the European Union Agency for Cybersecurity. (NIST, 2020a; NIST, 2020b; ENISA, 2024). The use of the simulation environment enabled safe and reproducible testing of scenarios that would be significantly limited in production systems.

To analyse the impact of spatial data quality on model behaviour, datasets with systematically differentiated quality parameters were prepared, including data completeness, positional accuracy, logical consistency, and attribute correctness as defined by ISO 19157-1:2023. Reference datasets were subjected to controlled degradation, and all variants were documented using metadata compliant with ISO 19115-1:2014. Several model classes representing different anomaly detection paradigms were used, including autoencoders, variational autoencoders, Isolation Forest, and graph neural networks taking into account topological relationships between spatial objects (Chandola et al., 2009). The purpose of the study was not to benchmark all available models, but to compare representative methodological classes relevant to the proposed framework.

The models were trained independently on datasets of different quality levels, and changes in their behaviour under controlled degradation conditions were observed. Model characteristics were determined based on anomaly detection metrics such as True Positive Rate and False Positive Rate, as well as model responses to anomaly injection. The reported results should be treated as measures of model behaviour in the simulation environment rather than as estimates of operational performance.

The resilience of AI models to geolocation manipulation was analysed using controlled GNSS attack scenarios, including gradual signal spoofing, slow position drift, coherent attacks involving simultaneous modification of multiple signal components, and training data poisoning scenarios (Psiaki & Humphreys, 2016; Bhatti & Humphreys, 2017; Humphreys et al., 2008).

Single-channel models based solely on GNSS observations were compared with metadata-enhanced and multimodal configurations integrating data quality descriptors and topological context. The analysis focused on changes in decision boundaries, the rate of prediction degradation, and the stability of results as manipulation intensity increased.

The impact of security architecture on geospatial service resilience was assessed in two variants of the service environment. The first variant represented a traditional architecture based on a trusted internal network, while the second implemented a Zero Trust architecture in accordance with NIST SP 800-207. OGC API – Features services were implemented in both configurations and tested against threat scenarios identified in the OWASP API Security Top 10, including Broken Object Level Authorization, Server-Side Request Forgery, query overload, and filtering parameter manipulation (OWASP Foundation, 2023; OGC, 2020). The responses of both architectures to the same classes of events, including incident detection time and degree of service degradation, were compared.

The selection of materials and methods was grounded in recognised standards and current engineering practice. ISO standards provided a formal apparatus for describing spatial data quality, OGC specifications defined an interoperable service architecture, and NIST documents together with ENISA reports provided structured threat scenarios and resilience principles (ISO, 2014; ISO, 2023; OGC, 2020; NIST, 2020a; NIST, 2020b; ENISA, 2024). Such a combination ensured methodological consistency with both regulatory and operational contexts.

The proposed approach has several limitations inherent to its simulation-based nature. Not all features of real-world GNSS attacks and complex production environments can be faithfully reproduced under laboratory conditions. The results should therefore be interpreted as an illustration of the potential of the proposed framework rather than as an empirical assessment of the resilience of specific GIS systems.

The research environment integrates data processing pipelines, AI analytics modules, and a GIS service layer. The input material includes synthetic GNSS data streams, topological and attribute data subjected to controlled qualitative degradation and described using ISO-compliant metadata. AI models analyse data in single-channel, metadata-enhanced, and multimodal configurations, enabling a comparative evaluation of their behaviour under simulated interference. The service layer includes OGC API –

Features in traditional and Zero Trust variants, and security modules implement attack scenarios in accordance with NIST and OWASP guidelines. The designed architecture ensures repeatability of experiments and allows future extension with additional models and threat scenarios.

A natural next stage of the proposed research would involve empirical validation using anonymised operational data obtained from public transport operators or municipal authorities. Such data could include GNSS trajectories, selected service logs, incident records, and API access patterns, provided that privacy-sensitive and security-sensitive elements are removed or aggregated. In that setting, the framework could be used to compare simulated resilience profiles with real operational anomalies, service disruptions, and security incidents.

The reported TPR and FPR values should be interpreted as aggregated indicators obtained within the simulation environment. In future extensions of the study, repeated simulation runs and formal reporting of variability measures, such as standard deviations or confidence intervals, should be incorporated to improve the statistical interpretability of the results. At the present stage, the emphasis is placed on methodological comparability rather than on full statistical generalisation.

Case study. The case study concerns an urban public transport system (PTS), used here as a reference environment to illustrate the proposed method for assessing the resilience of GNSS data and GIS services to cyber threats. PTS was selected because of its high operational complexity, continuous generation of high-frequency spatial data, and significant exposure to data quality disruptions and information attacks. In the analysed model, each vehicle (bus or tram) reports GNSS position data at intervals ranging from one to several seconds. These observations are then processed, validated, and published through services compliant with the OGC API – Features standard. The system performs key urban functions, including traffic monitoring, traffic control support, passenger information, and punctuality analysis.

The case study is not intended as a full empirical validation of model performance; rather, it provides a structured demonstration environment showing how assumptions A1–A3 can be operationalised in a realistic GIS context, in accordance with methodological approaches recommended, among others, by the National Institute of Standards and Technology (NIST, 2020a; NIST, 2020b).

The first element of the case study consists of GNSS reference trajectories, which include time-ordered observations of vehicle position, geographic coordinates, timestamps, signal quality parameters, and movement speed. On this basis, spatial data quality profiles in accordance with ISO 19157-1:2023 were defined to operationalise research assumption A1 concerning the impact of input data quality on the stability and interpretability of analytical models. Four data quality profiles were distinguished: high (BH), medium (BM), low (BL), and low with topological perturbations (BLT), as listed in Table 1.

Table 1. Spatial data quality profiles in accordance with ISO 19157-1

Profile	Mean horizontal error (m)	Data gaps (%)	Topology violations (%)	Mean HDOP	Median satellites
BH	0.7	0.2	0.0	0.9	10
BM	1.9	1.1	0.1	1.4	8
BL	3.8	4.9	0.3	2.1	6
BLT	3.6	4.5	1.6	2.0	6

Source: own study

These profiles differ with respect to mean positional error, data gaps, topology violations, and selected GNSS signal quality parameters. Figure 1 summarises the progression of degradation across the BH, BM, BL, and BLT profiles and provides the basis for subsequent comparisons of model behaviour.

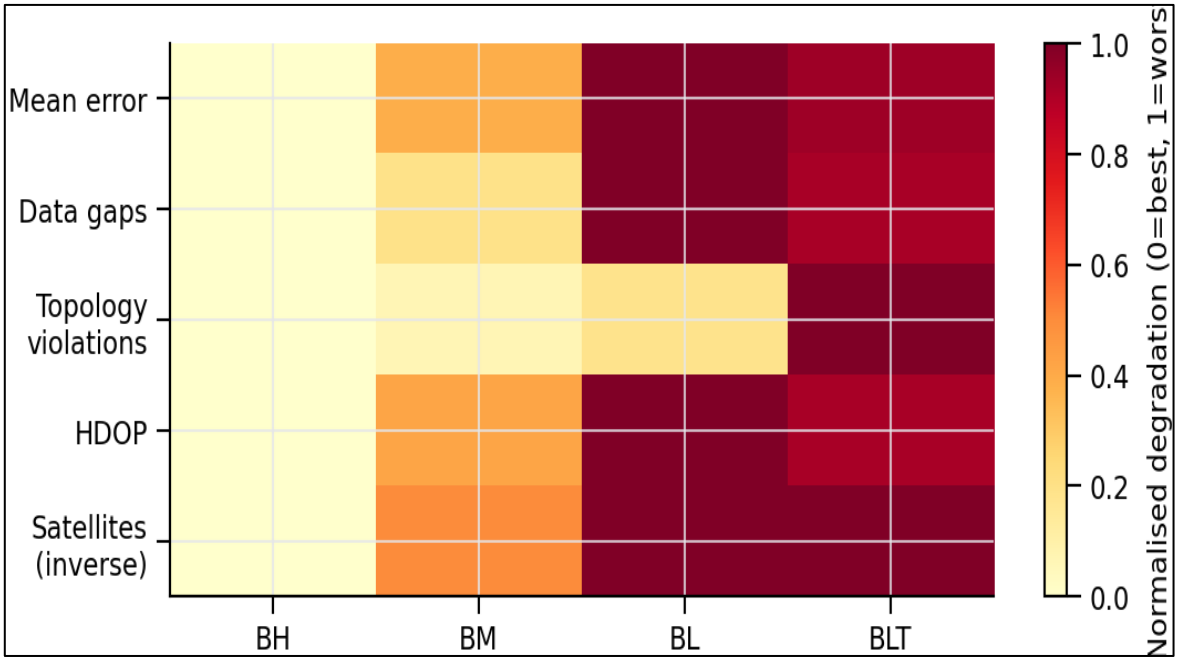

Fig. 1. Comparison of spatial data quality profiles (BH, BM, BL, and BLT) based on selected indicators defined in Table 1: mean horizontal error, data gaps, topology violations, mean HDOP, and median number of satellites
Source: own elaboration

The second element of the case study consists of GNSS signal manipulation scenarios designed to illustrate research assumption A2, concerning the resilience of analytical methods and AI models to intentional disturbances of location data. Two classes of spoofing scenarios were prepared: an increasing-drift scenario and a jump-attack scenario. A sample of the increasing-drift scenario is presented in Table 2.

Table 2. Sample GNSS spoofing data under an increasing drift scenario

Time (UTC)	Actual position	Spoofed position	Deviation (m)
08:19:00	52.23201 / 21.01314	52.23201 / 21.01314	0.00
08:19:02	52.23215 / 21.01349	52.23213 / 21.01346	0.35
08:19:04	52.23228 / 21.01383	52.23224 / 21.01378	0.71
08:19:06	52.23241 / 21.01416	52.23234 / 21.01408	1.12

Source: own elaboration

Figure 2 illustrates the increasing-drift GNSS spoofing scenario by showing the gradual growth of position deviation over time in the synthetic transport trajectory.

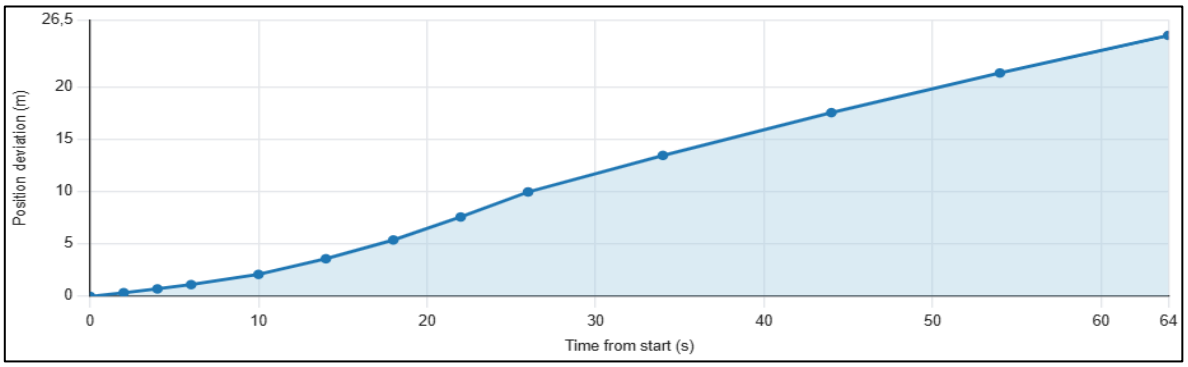

Fig. 2. GNSS spoofing scenario with increasing drift: position deviation over time for the synthetic urban public transport trajectory
Source: own elaboration

Jump attacks generate abrupt position shifts of substantial magnitude while preserving the apparent plausibility of the trajectory. These scenarios were selected based on established GNSS threat models described in the literature and should be treated as a reference set rather than a reconstruction of any specific operational incident (Psiaki & Humphreys, 2016; Bhatti & Humphreys, 2017; Humphreys et al., 2008; Jafarnia-Jahromi et al., 2012).

Another component of the case study is a synthetic but operationally realistic set of API call logs for spatial publishing services, covering both legitimate traffic and requests classified as potentially abusive. This data was prepared to illustrate research assumption A3, according to which the security architecture of the service layer significantly affects the resilience and stability of GIS services made available through APIs. The logs were generated for two contrasting service architectures: a traditional trust-based architecture and a Zero Trust architecture.

Figure 3 provides a comparative view of API response times by request class in the traditional and Zero Trust architectures used in the simulated geospatial service environment.

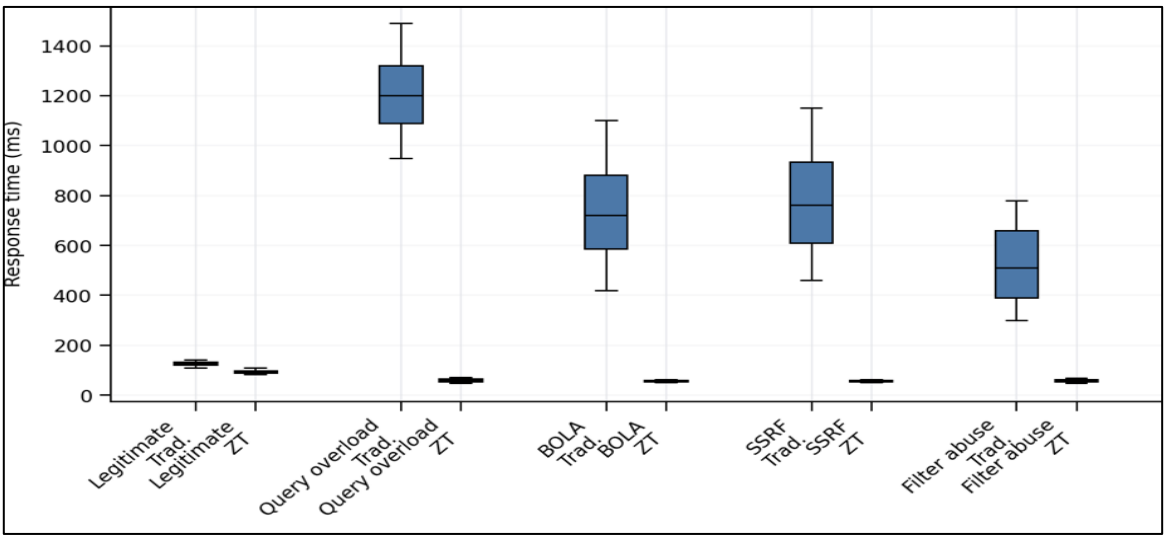

Fig. 3. Distribution of API response times by request class in the traditional and Zero Trust architectures for the simulated geospatial service environment
Source: own elaboration

Figure 4 summarises the proportions of successfully processed legitimate requests and blocked abusive requests in the traditional and Zero Trust architectures analysed in the case study.

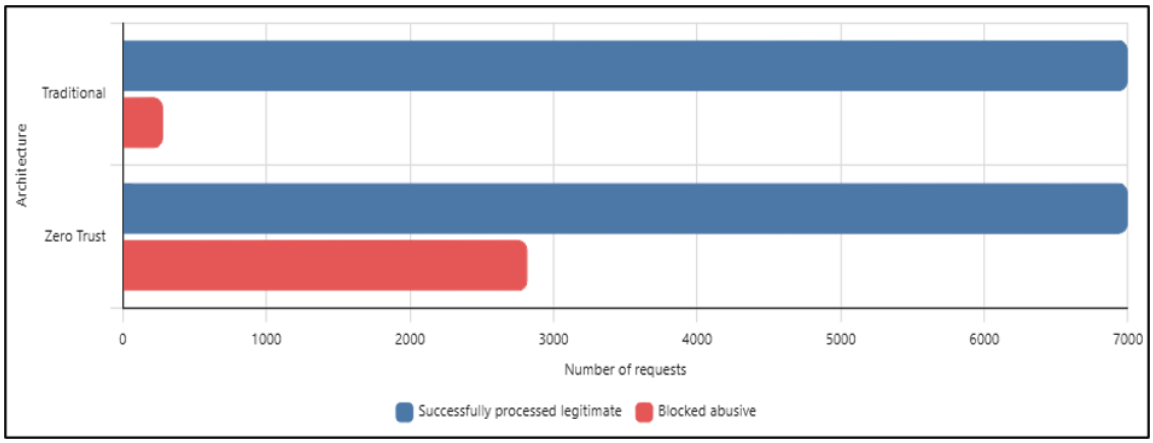

Fig. 4. Comparison of successfully processed legitimate requests and blocked abusive requests in the traditional and Zero Trust API architectures
Source: own elaboration

The presented logs and visualisations provide the basis for the analysis developed in the following section, which evaluates the impact of security architecture on the effectiveness of abuse prevention, response-time stability, and the resilience of OGC API services to simulated attack scenarios.

Due to the limited availability of real-world operational data and the need to ensure replicability of analyses, all datasets used in this case study are synthetic. They were generated based on typical operating parameters of urban GNSS systems, error ranges and non-observations reported in the literature, and known classes of attack and disruption scenarios. The data generation procedure included defining reference

trajectories, imposing controlled quality degradation, simulating geolocation manipulations, and generating API traffic logs according to specified workload profiles and security policies.

The presented case study provides a structured reference environment for the analyses in the next section. The data, tables, and figures are not treated as empirical results, but as a demonstration tool allowing consistent reference to assumptions A1–A3, comparability of scenarios, and assessment of the usefulness of the proposed framework in a realistic GIS context.

Results and discussion

The results reported in this section are based on the synthetic spatiotemporal datasets and OGC API service call logs introduced in the Case Study section and are intended to demonstrate the analytical applicability of the proposed framework under controlled conditions. The use of synthetic data made it possible to control data quality degradation, attack intensity, and service-layer abuse scenarios while preserving the operational realism of an urban public transport setting. The analyses were conducted in accordance with the procedures described in the Materials and Methods section and were designed to examine research assumptions A1–A3.

The relationship between spatial data quality and anomaly detection performance was analysed using the four quality profiles defined in Table 1, namely BH, BM, BL, and BLT. These profiles provided the basis for generating training and test datasets used to evaluate the analysed model configurations. The relationship between spatial data quality and model behaviour is examined with reference to Figure 1 and to Figures 5–7, which provide complementary views of anomaly detection performance.

Figure 5 presents the effect of spatial data quality on anomaly detection sensitivity by comparing True Positive Rate (TPR) values across the BH, BM, BL, and BLT profiles.

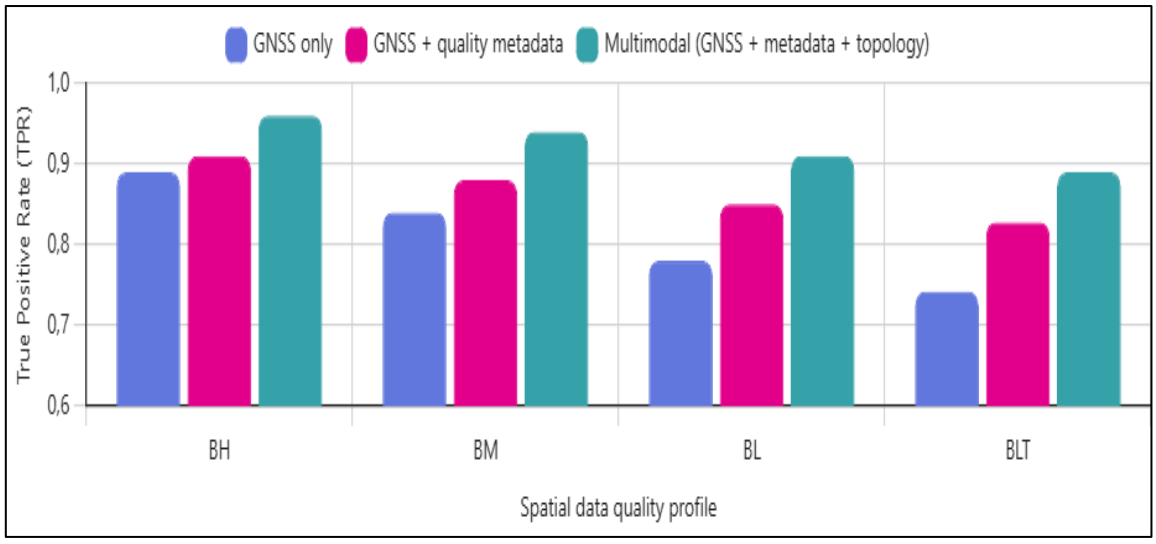

Fig. 5. True Positive Rate (TPR) of anomaly detection model configurations across the spatial data quality profiles BH, BM, BL, and BLT
Source: own elaboration

The analysis reveals substantial performance differences across model configurations, particularly under degraded data quality conditions. Information-rich models consistently outperformed single-channel models in both detection accuracy and robustness. For all quality profiles, a systematic advantage of more information-rich models over single-channel models was observed. The average True Positive Rate increased from 0.813 for the GNSS-only configuration to 0.867 for the configuration using quality metadata and to 0.925 for the multimodal configuration that additionally considers topological context. These differences were particularly pronounced for the BL and BLT profiles, where degradation of data quality was greatest. These results support research assumption A1 and indicate that the formal treatment of spatial data quality significantly affects anomaly detection stability and accuracy (ISO, 2023; Longley et al., 2015).

Figure 6 complements the TPR analysis by showing the False Positive Rate (FPR) obtained for each model configuration across the BH, BM, BL, and BLT spatial data quality profiles.

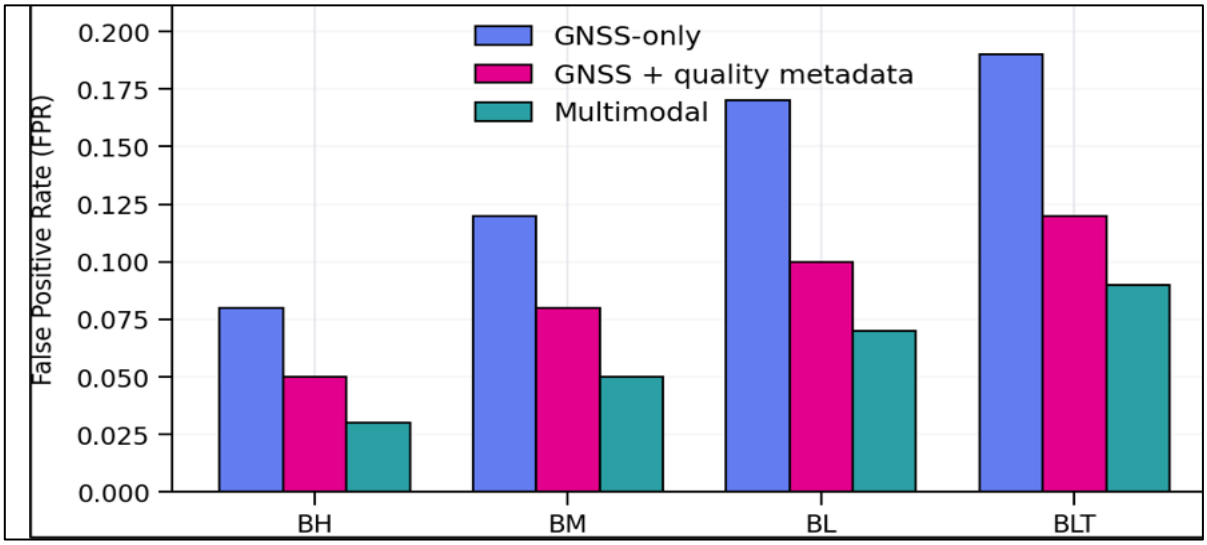

Fig. 6. False Positive Rate (FPR) of anomaly detection model configurations across the spatial data quality profiles BH, BM, BL, and BLT
Source: own elaboration

Lower spatial data quality is associated with higher False Positive Rate values, particularly in less information-rich model configurations. The average FPR decreased from 0.140 for the single-channel configuration to 0.0875 for the metadata-based configuration and to 0.060 for the multimodal configuration. The greatest reduction in false positives was observed under low-quality data conditions, indicating that explicit consideration of data quality and metadata reduces model hypersensitivity to input interference. This suggests that data quality control should be treated as an operationally important component of GIS systems using artificial intelligence methods.

Figure 7 provides a ROC-like comparison of the analysed model configurations, enabling an overall assessment of detection effectiveness across the simulation scenarios.

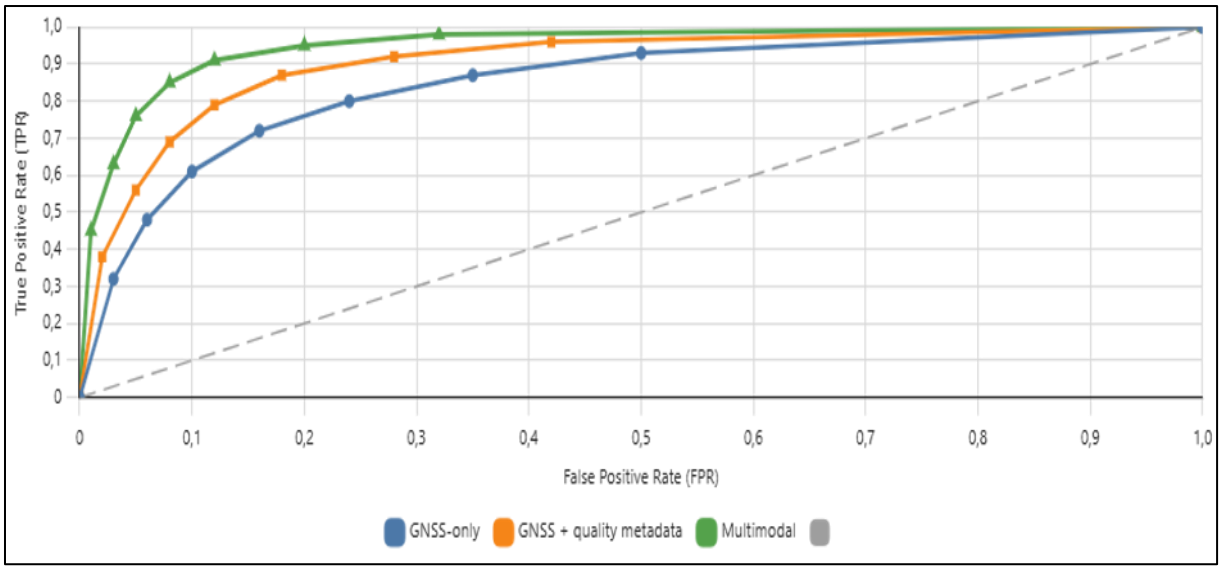

Fig. 7. ROC-like comparison of anomaly detection model configurations used in the simulation environment
Source: own elaboration

The comparison shows that the multimodal configuration achieves the most favourable balance between detection sensitivity and false-positive control, whereas less information-rich configurations exhibit weaker overall performance. Taken together, Figures 5–7 indicate that the performance advantage of richer analytical configurations remains stable across multiple views of model behaviour and is not limited to a single evaluation metric.

The resilience of AI models to GNSS signal manipulation was further examined using the slow-drift and step-displacement scenarios described in the Case Study section. In the drift variant, the position deviation reached 10 m after about 26 s and 25 m after about 64 s from the start of the sequence. Under operational conditions, such deviations may gradually distort inference related to punctuality assessment, route adherence, or prioritisation in traffic control systems. The simulation results indicate that multimodal models remain more stable under such conditions than single-channel configurations, particularly when data quality is degraded.

More specifically, multimodal models integrating positional data, quality metadata, and topological context maintained high effectiveness, with TPR values in the range of 0.88–0.97 while reducing FPR values to approximately 0.03–0.09. In contrast, single-channel models showed a marked decline in effectiveness and an increase in false positives, especially under reduced data quality conditions. These results support research assumption A2 and indicate that multimodality is a principal factor increasing the resilience of AI models to geolocation manipulation.

The impact of security architecture on the resilience of geospatial services was assessed by comparing two variants of the OGC API architecture defined in the case study: traditional architecture and a Zero Trust architecture. The analysis was based on API call logs and security policy enforcement signals, and the aggregated results are shown in Figures 3 and 4. In the traditional architecture, unwanted load tests most often resulted

in HTTP 200 responses with a median response time of approximately 1.2 s, whereas in the Zero Trust architecture similar attempts were limited at an early processing stage, resulting in HTTP 429 responses and response times of approximately 60 ms. Similar patterns were observed for Broken Object Level Authorization (BOLA) and Server-Side Request Forgery (SSRF) violations (OWASP Foundation, 2023).

In the Zero Trust architecture, these attempts were consistently blocked at response times of approximately 55–57 ms, while in the traditional architecture they led to long response times or server-side errors. A cumulative comparison of the proportion of blocked requests indicates that about 2.8% of requests were blocked in the traditional variant, whereas in the Zero Trust architecture this percentage was about 28.2%. At the same time, the median response time for legitimate queries decreased from around 127 ms to around 93 ms, indicating that the use of a Zero Trust architecture does not degrade service quality for authorized API users, but instead promotes service stability.

Overall, the findings indicate that GIS cyber resilience is not determined by a single component. Rather, it emerges from the interaction between data quality, AI model robustness, and service-layer security architecture. Analysis of these dimensions in isolation is insufficient, whereas their integrated consideration allows for a coherent and measurable assessment of the security posture of modern GIS systems. The obtained results remain consistent with research assumptions A1–A3 and support the rationale for designing geoinformation systems as integrated ecosystems in which individual security layers complement one another.

Unless stated otherwise, the reported performance indicators should be interpreted as aggregated values obtained within the simulation setting. In future extensions of the framework, repeated simulation runs and formal variability measures, such as standard deviations or confidence intervals, should be reported to improve the statistical interpretability of model comparisons. At the present stage, the emphasis remains on methodological comparability rather than on full statistical generalization.

Conclusions

This paper presents an integrated methodological perspective on the role of artificial intelligence in the cybersecurity of modern GIS systems, combining geospatial data quality, analytical model resilience, and service-layer security architecture. The adopted research approach, based on a simulation-scenario environment and synthetic data with realistic parameters, enabled a consistent demonstration of the relationships among these areas without claiming full empirical validation in an operational implementation setting.

The results confirm that the quality of spatial data is a key factor determining the stability and reliability of AI-based analyses. High-quality data, formally described in accordance with ISO standards for data quality and metadata, helps to maintain high accuracy in anomaly detection and reduce false positives. Under conditions of data quality degradation, a significant decrease in the effectiveness of single-channel approaches was

observed, indicating that data quality management should be treated as an integral part of the GIS system lifecycle rather than merely as a preprocessing step.

An important conclusion from the analysis of model resilience to geolocation manipulation is the clear advantage of multimodal approaches over models based solely on raw GNSS observations. The integration of positional information with data quality metadata and topological context increases resilience to both gradual and abrupt GNSS spoofing scenarios. These findings indicate that multimodality is not merely an algorithmic improvement, but a condition for the correct operation of detection systems in environments exposed to intentional interference with location data.

In parallel, the analysis of the service layer showed that a security architecture based on the Zero Trust paradigm significantly increases the resilience of geospatial services provided through OGC APIs to common classes of abuse, including privilege escalation, query overloads, and indirect attacks. Importantly, the improvement in security was not associated with a deterioration in the quality of processing legitimate requests but rather contributed to stabilizing response times and reducing the impact of unwanted traffic on service availability.

A comprehensive interpretation of the results leads to the conclusion that the resilience of spatial information systems to modern cyber threats is emergent and results from the interaction among data quality, analytical model resilience, and service-layer security architecture. Analysis of these areas in isolation is insufficient, whereas their integrated consideration enables a coherent and measurable assessment of the security of modern geoinformation systems.

The proposed framework provides a foundation for future empirical research, particularly studies based on operational data, extended attack taxonomies, and more advanced approaches to AI interpretability and auditability (NIST, 2023; ISO/IEC, 2023; European Parliament & Council of the European Union, 2025). A particularly important next step will be validation of the framework using anonymised operational datasets from public transport environments, including real GNSS trajectories, service logs, and incident-related records.

Overall, the paper provides a coherent case for designing GIS systems as integrated ecosystems in which data quality, analytical methods, and security architecture complement one another.

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

Bhatti J., Humphreys T.E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. Navigation, 64(1), 51–66.

Chandola V., Banerjee A., Kumar V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.

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

European Parliament and Council of the European Union (2007). Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

European Parliament and Council of the European Union (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2).

European Parliament and Council of the European Union (2025). Artificial Intelligence Act (AI Act).

Goodchild M.F. (2010). Twenty years of progress: GIScience in 2010. Journal of Spatial Information Science, 1(1), 3–20.

Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner P.M. Jr. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In: Proceedings of ION GNSS 2008, 2314–2325.

IEC (2024). International Electrotechnical Commission. IEC 62443-2-1:2024 – Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners. IEC, Geneva.

ISO (2014). International Organization for Standardization. ISO 19115-1:2014 – Geographic information – Metadata – Part 1: Fundamentals.

ISO (2023). International Organization for Standardization. ISO 19157-1:2023 – Geographic information – Data quality – Part 1: General requirements.

ISO/IEC (2022). International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27001:2022 – Information security management systems – Requirements.

ISO/IEC (2023). International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 23894:2023 – Artificial intelligence – Guidance on risk management.

Jafarnia-Jahromi A., Broumandan A., Lin T., Lachapelle G. (2012). A cognitive approach for GPS signal authentication: A review. GPS Solutions, 16(4), 485–497.

Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W. (2015). Geographic Information Science and Systems. 4th ed. Wiley.

NIST (2020a). National Institute of Standards and Technology. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations.

NIST (2020b). National Institute of Standards and Technology. NIST Special Publication 800-207: Zero Trust Architecture.

NIST (2023). National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0).

OGC (2020). Open Geospatial Consortium. OGC API – Features – Part 1: Core.

OGC (2021). Open Geospatial Consortium. OGC API – Features – Part 3: Coordinate Reference Systems by Reference.

OGC (2022). Open Geospatial Consortium. OGC API – Features – Part 2: Filtering.

OWASP Foundation (2023). OWASP API Security Top 10 – 2023.

Psiaki M.L., Humphreys T.E. (2016). GNSS spoofing and detection. Proceedings of the IEEE, 104(6), 1258–1270.