GIS Odyssey Journal

2026 • Volume 6 • Number 2

https://doi.org/10.57599/gisoj.2026.6.2.89

Jerzy Stanik[1], Kazimierz Worwa[2]

USE OF ARTIFICIAL INTELLIGENCE IN CYBER THREAT DETECTION AND GEOSPATIAL DATA INTEGRITY PROTECTION IN GIS ENVIRONMENTS

Abstract: The development of Geographic Information Systems (GIS), cloud services, Internet of Things technologies and artificial intelligence has increased the operational importance of geospatial data. At the same time, enterprises using GIS face cyber threats that may disrupt not only IT infrastructure, but also the integrity of spatial data used in decision-making. This article evaluates the effectiveness of artificial intelligence in cyber threat detection and geospatial data integrity protection. The study is based on a single case study of a medium-sized enterprise using GIS, GPS, IoT and SIEM infrastructure. A traditional rule-based system was compared with an AI-supported architecture using quantitative indicators: classification accuracy, precision, Recall, F1-score, false positive rate, mean detection time, integrity violation detection rate and the proposed GIS Integrity Index. The empirical description was supplemented with aggregated operational values adopted as expert-based validation assumptions within the case-study protocol. These values were used to increase methodological transparency, clarify the comparative procedure, and ensure consistent interpretation of the results obtained for the traditional and AI-supported systems. The results indicate improved threat detection and data integrity monitoring following the implementation of AI mechanisms. In the validation set with controlled label consistency, classification accuracy increased from 83.4% to 95.8%, Recall from 80.1% to 95.5%, IDR from 68% to 95%, and GII from 0.91 to 0.98. The findings should be interpreted in the context of a single case study and require further validation in other organizational environments.

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

Received: 30 June 2026; accepted: 18 July 2026; revised: 4 August 2026

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-0162-2579, email: jerzy.stanik@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 digital transformation of enterprises has increased the volume, velocity and strategic importance of data used in operational and managerial processes. Geospatial data are especially important in transport, logistics, energy, critical infrastructure, municipal management, spatial planning and environmental monitoring. As a result, Geographic Information Systems (GIS) have become a key component of enterprise information infrastructure (Longley et al., 2015; Duckham et al., 2023).

GIS environments integrate data from spatial databases, GPS, IoT sensors, monitoring systems and business applications. These data support analyses, maps, reports and operational decisions. However, their growing importance increases requirements related to quality, reliability, cybersecurity and integrity (Longley et al., 2015; Duckham et al., 2023; ISO, 2023).

Cybersecurity threats increasingly involve not only unauthorized access to information, but also manipulation of data, modification of records and long-term degradation of data quality. Such attacks are particularly dangerous in GIS environments because small changes in object geometry, attributes or topology may lead to incorrect spatial analyses and wrong operational decisions (ENISA, 2024; NIST, 2024; Kiedrowicz, 2025).

Traditional security systems rely on expert rules, known signatures and static policies. This approach remains useful, but its effectiveness decreases against new attacks, insider actions and subtle modifications of data. In large and dynamic GIS environments, manual or rule-based monitoring is insufficient for detecting complex anomalies (ENISA, 2024; Buczak & Guven, 2016; Panigrahi et al., 2021).

Artificial intelligence and machine learning can support cybersecurity by identifying patterns, classifying suspicious events, detecting anomalies and monitoring user activity. In GIS environments, AI may also support the continuous assessment of attribute accuracy, topology correctness and data completeness (Buczak & Guven, 2016; Chandola et al., 2009; Panigrahi et al., 2021).

The research gap addressed in this article concerns the integrated assessment of AI-supported cyber threat detection and geospatial data integrity protection in an enterprise GIS environment. Existing studies often focus on network intrusion detection or general GeoAI, while less attention is paid to the relationship between cyber events and the integrity of spatial data resources (Janowicz et al., 2020; Duckham et al., 2023; ISO, 2023).

The purpose of this article is to evaluate the use of artificial intelligence in cyber threat detection and geospatial data integrity protection in an enterprise using GIS. The main research question is: How does artificial intelligence affect cyber threat detection effectiveness and the protection of geospatial data integrity in an enterprise GIS environment?

The research hypothesis, treated as an applied case-study hypothesis, is that AI algorithms are expected to increase cyber threat detection effectiveness and improve geospatial data integrity protection compared with traditional rule-based and signature-based security mechanisms. The hypothesis is therefore assessed analytically within the

investigated case rather than statistically verified for a general population of GIS-based enterprises.

The article makes three contributions. First, it proposes an integrated evaluation approach that links cyber threat detection indicators with geospatial data integrity indicators. Second, it introduces the GIS Integrity Index as a composite indicator for assessing attribute accuracy, topological correctness and data completeness in a cybersecurity context. Third, it presents a case-study comparison of a traditional rule-based monitoring approach and an AI-supported approach in an enterprise GIS environment.

The study is intentionally positioned as an applied case study. Its goal is not to claim universal effectiveness of a single AI model, but to show how AI-supported monitoring can be evaluated when geospatial data integrity is treated as a cybersecurity objective. This distinction is important because many GIS-related incidents may not appear as classical network attacks but may still degrade the reliability of spatial analyses and decisions.

The case-study character of the research means that the results should be interpreted as evidence from one enterprise environment rather than as statistically generalisable evidence for all GIS-based enterprises. The purpose of the case study is analytical and methodological: to show how cyber threat detection indicators can be jointly assessed with geospatial data integrity indicators.

The remainder of the article is structured as follows: the research design, data sources, evaluation indicators and experimental assumptions; the investigated enterprise and implementation context; the results; the findings in relation to the research hypothesis and the operational context of the case study; practical implications, limitations and future research directions; the main conclusions.

Materials and methods

Research objective. The objective of the research was to evaluate the effectiveness of artificial intelligence in cyber threat detection and in the protection of geospatial data integrity. The study focused on the ability of machine learning mechanisms to identify cyber incidents affecting spatial data and to support continuous monitoring of GIS data quality.

Research problems and hypothesis. The research problem was formulated as follows: How does the application of artificial intelligence influence cyber threat detection effectiveness and geospatial data integrity protection in an enterprise using GIS? The hypothesis was examined within the case-study setting by comparing a traditional rule-based security system with an AI-supported system integrating SIEM data, user activity, network events and changes in GIS databases.

Research subjects and objects. The subject of research included cyber threat detection processes and mechanisms for protecting the integrity of geospatial data. The research object was a medium-sized enterprise using GIS data in business, operational and analytical processes. The investigated environment included GIS

platforms, relational spatial databases, GPS devices, IoT sensors, a SIEM system, network infrastructure and AI analytical modules.

Research material. The research material included system and application logs, network logs, SIEM events, user activity history, geospatial data stored in GIS databases, GPS location data, IoT sensor data and registered security incidents. The analysis focused on events that could affect object coordinates, spatial attributes, topology relationships, data completeness or unauthorized data export.

Nature of empirical data and validation assumptions. The study combines three categories of information: observed case-study data, aggregated operational indicators and expert-based validation assumptions. Observed data include registered security incidents, GIS database change records and confirmed integrity-related events available within the investigated enterprise. Aggregated operational indicators describe the scale of the analysed environment without disclosing sensitive infrastructure details. Expert-based validation assumptions were introduced only where full operational disclosure was not possible, in order to make the evaluation framework transparent and internally consistent. Therefore, the reported quantitative results should be interpreted as case-study evaluation results supported by expert-based validation assumptions, not as statistically generalisable findings. The scope and validation assumptions of the empirical material are summarized in Table 1, which clarifies the scale of the case-study dataset before the analytical procedure is described.

Table 1. Aggregated case-study dataset characteristics and validation assumptions

Dataset element	Aggregated value adopted in the case-study protocol	Role in the study
Observation period	6 months, January-June 2026	Defines the before/after and validation context
Registered SIEM and system events	12,480 events	Source for cybersecurity event screening
GIS database change records	2,360 records	Source for geometry, attribute and topology monitoring
GPS/IoT records	48,500 records	External data streams for spoofing and anomaly checks
Active system users	38 users	Population for behavioural profiling
Users with GIS editing rights	14 users	Population for GIS modification analysis
Monitored GIS objects	128,000 objects	Reference base for integrity monitoring
Labelled event windows for classifier validation	1,033 windows	Input for confusion-matrix-based evaluation
Incident-class event windows	447 windows	Positive class in validation
Normal event windows	586 windows	Negative class in validation
Confirmed operational security incidents	144 incidents	Incident structure reported in the Results section

Source: own elaboration based on aggregated case-study indicators and expert-based validation assumptions adopted within the case-study protocol

The values in Table 1 are not disclosed raw operational counts. They are aggregated case-study indicators and expert-based validation assumptions used to describe the scale and logic of the evaluation framework. They should therefore be interpreted within the limits of a single case-study design and not as statistically representative for all GIS-based enterprises.

Research methods. The study used a structured case-study protocol, literature review, comparative analysis and quantitative assessment. The literature review was used to identify the state of knowledge on AI in cybersecurity, GIS and geospatial data quality. The case-study protocol enabled systematic analysis of a real enterprise environment and comparison of two security architecture variants: traditional rule-based monitoring and AI-supported monitoring (Buczak & Guven, 2016; Panigrahi et al., 2021; Janowicz et al., 2020; ISO, 2023).

Case-study protocol. The research procedure followed seven stages: identification of relevant cybersecurity and GIS data sources; extraction of event and data-change records; preprocessing and time alignment; expert-supported labelling of integrity-related events; configuration of the traditional and AI-supported analytical variants; comparative evaluation using common validation windows; and interpretation of results in relation to geospatial data integrity indicators. This protocol was adopted to ensure that both system variants were assessed using the same categories of events, the same evaluation logic and a consistent set of validation assumptions.

Artificial intelligence methods used in the study. The AI component combined supervised and unsupervised analytical mechanisms. Supervised classification was used to distinguish potentially harmful events from normal activity, while anomaly detection was used to identify atypical user behaviour and unusual modifications in GIS databases (Buczak & Guven, 2016; Chandola et al., 2009; Panigrahi et al., 2021). The study assumed a hybrid approach consisting of event classification, anomaly detection, user activity analysis and GIS change monitoring (Buczak & Guven, 2016; Chandola et al., 2009; Panigrahi et al., 2021).

Because the investigated enterprise environment contains security-sensitive information, the description is presented at an aggregated methodological level without disclosing product names, detailed infrastructure parameters or sensitive operational identifiers. The traditional system and the AI-supported system were evaluated on the same labelled event windows so that the comparison focused on the added analytical value of AI rather than on differences in data availability.

The validation procedure used a stratified train-validation-test split. Because cybersecurity datasets are typically imbalanced, class weighting was applied in the supervised classifier. The validation subset was used for model selection and parameter tuning, while the test subset was reserved for final comparison between the traditional and AI-supported variants. To reduce data leakage, event windows associated with the same incident sequence were not split between training and testing subsets. The analytical structure of the AI-supported evaluation is specified in Table 2, linking each task with its data sources, modelling mechanism, validation logic and output.

Table 2. Integrated analytical tasks, data sources, models and validation logic

Analytical task	Main data sources	Model / mechanism	Validation logic	Output
Security event classification	SIEM events, system logs, user activity windows	Random Forest classifier with class weighting	Stratified 60/20/20 train-validation-test split; validation subset used for model tuning	Suspicious event class and probability score
Anomaly detection	GIS change records, user activity windows, GPS/IoT streams	Isolation Forest with contamination parameter set at 0.05	Expert-confirmed abnormal patterns used for validation; event-window separation used to reduce leakage	Anomaly score and anomaly flag
User activity analysis	Login time, access path, editing frequency, modification history	Behavioural baseline and deviation scoring	Comparison with normal user profiles derived from the observation period	User deviation score and risk category
GIS integrity monitoring	Coordinates, attributes, topology relations, completeness indicators	Rule-based topology checks combined with ML-supported anomaly scoring	Expert review of coordinate shifts, attribute changes and topology violations	Integrity risk category and inputs to GII/IDR
Model governance	Training logs, validation metrics, model versions	Grid search, model registry and leakage-control procedures	Best configuration selected on validation subset, final indicators reported on common validation windows	Auditable model configuration and evaluation trace

Source: own elaboration based on the case-study protocol and expert-based validation assumptions

For methodological completeness, the AI-supported architecture is described through analytical tasks, data sources, model families, validation logic and expected outputs. Because the investigated enterprise environment contains security-sensitive information, the description remains aggregated and does not disclose product names, detailed infrastructure parameters or sensitive operational identifiers.

Effectiveness evaluation criteria. Cyber threat detection was evaluated using standard classification indicators: Accuracy, Precision, Recall and F1-score. These measures are commonly used to evaluate classifiers in intrusion detection and cybersecurity monitoring (Buczak & Guven, 2016; Panigrahi et al., 2021).

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (1)$$

$$\text{Precision} = TP / (TP + FP) \quad (2)$$

$$\text{Recall} = TP / (TP + FN) \quad (3)$$

$$F1 = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall}) \quad (4)$$

Geospatial data integrity was evaluated using the GIS Integrity Index (GII), proposed in this study as a domain-specific composite indicator. It combines attribute accuracy (A), logical/topological consistency (T) and data completeness (C), which are key aspects of geographic data quality and correspond to the ISO 19157-1:2023 framework for describing, evaluating and reporting geographic data quality (ISO, 2023). The calculation

logic for the classification indicators is illustrated in Table 3, which presents the consistency-control confusion matrix used in the validation framework.

Table 3. Consistency-control confusion matrix used to illustrate the validation framework

System variant	TP	TN	FP	FN	Accuracy	Precision	Recall	F1-score	FPR
Traditional rule-based system	358	504	82	89	83.4%	81.4%	80.1%	80.7%	14.0%
AI-supported system	427	563	23	20	95.8%	94.9%	95.5%	95.2%	3.9%

Source: own elaboration based on expert-based validation assumptions adopted within the case-study protocol; values serve as consistency-control assumptions for demonstrating the evaluation framework

The values in Table 3 are used as consistency-control values to demonstrate the calculation logic of the evaluation indicators. They support the internal coherence of the case-study comparison but should not be interpreted as independently audited operational measurements or statistically generalisable validation results.

$$GII = \alpha A + \beta T + \gamma C, \text{ where } \alpha + \beta + \gamma = 1 \quad (5)$$

The weights used in the GIS Integrity Index were determined through expert assessment conducted within the case-study protocol. Attribute accuracy received the highest weight because descriptive attributes were directly used in operational decisions. Logical/topological consistency received the second highest weight due to its importance in network and infrastructure analyses. Data completeness was assigned to a lower, but still significant, weight because missing data were generally easier to identify than subtle attribute or topology modifications. The adopted weights were $\alpha = 0.40$, $\beta = 0.35$ and $\gamma = 0.25$. The GII should be interpreted as a domain-specific indicator that requires recalibration in other organizational environments. A sensitivity analysis is recommended in future work. For this case-study version, the expert-defined weighting scheme is used only to demonstrate the integrated cybersecurity and GIS-quality assessment logic. The expert rationale for the GIS Integrity Index weighting scheme is detailed in Table 4, explaining how the weights assigned to the GII components were justified.

Table 4. Expert-based weighting logic for the GIS Integrity Index

GII component	Weight	Expert rationale
Attribute accuracy A	0.40	Operational decisions depend strongly on descriptive attributes of GIS objects
Logical/topological consistency T	0.35	Network and infrastructure analyses require correct spatial relationships
Data completeness C	0.25	Missing records is important but usually easier to detect than subtle manipulation
Total	1.00	Weights sum to 1.00 as required by the GII formula

Source: own elaboration based on expert assessment conducted within the case-study protocol

Sensitivity of the GIS Integrity Index. Because the GII uses expert-defined weights, a sensitivity analysis is required to assess whether the interpretation depends strongly on the adopted weighting scheme. In this case-study version, the adopted weights reflect the operational importance of attribute accuracy, logical/topological consistency, and data completeness. Future validation should compare alternative weighting scenarios, including equal weights, attribute-dominant weights and topology-dominant weights. Alternative weighting assumptions for the GIS Integrity Index are presented in Table 5 to indicate how future sensitivity analysis may be structured.

Table 5. Sensitivity scenarios for GIS Integrity Index weighting

Scenario	A weight	T weight	C weight	Purpose
Adopted case-study weights	0.40	0.35	0.25	Operational decision support
Equal weights	0.33	0.33	0.34	Neutral benchmark
Topology-dominant weights	0.30	0.50	0.20	Infrastructure and network analysis
Completeness-sensitive weights	0.35	0.30	0.35	Data-availability-oriented scenario

Source: own elaboration based on the proposed sensitivity-analysis logic for GII

$$IDR = (Nw / Nc) \times 100\% \quad (6)$$

In the IDR formula, Nw is the number of detected integrity violations and Nc is the total number of confirmed integrity violations.

Research model. The research model consisted of data collection, preprocessing, AI-based analysis, classification and anomaly detection, integrity assessment, alert generation and result interpretation. The model followed the logic of information security management and cyber risk assessment (ISO/IEC, 2022; NIST, 2024).

Figure 1 presents the complete conceptual research model. The empirical comparison reported in this article focuses on the data collection, preprocessing, AI-based analysis, threat and integrity detection, and evaluation stages. The response, remediation and feedback components are included to show the operational context of the proposed approach, but they are not evaluated as separate empirical modules in this study.

Empirical dataset and experimental configuration. To strengthen the repeatability of the study, the empirical setting was defined as follows. The dataset covered SIEM events, system logs, user activity records, GIS database change logs, GPS records and IoT measurements collected during the analysed observation period. Events were screened for relevance to cybersecurity and geospatial data integrity. Confirmed incidents were verified by cybersecurity and GIS domain experts. The same test scenarios and event categories were used to compare the traditional rule-based system and the AI-supported system.

The traditional system was defined as a rule-based and signature-based security monitoring solution operating within the SIEM platform. It relied on predefined correlation rules, access policies, known attack signatures and threshold-based alerts. It did not automatically model normal geospatial data change patterns. The AI-supported system extended this architecture with machine learning modules for classification, anomaly detection and geospatial integrity assessment. The overall research model is

visualized in Figure 1 to show how data collection, AI analysis, integrity assessment and operational response are connected in the case-study framework.

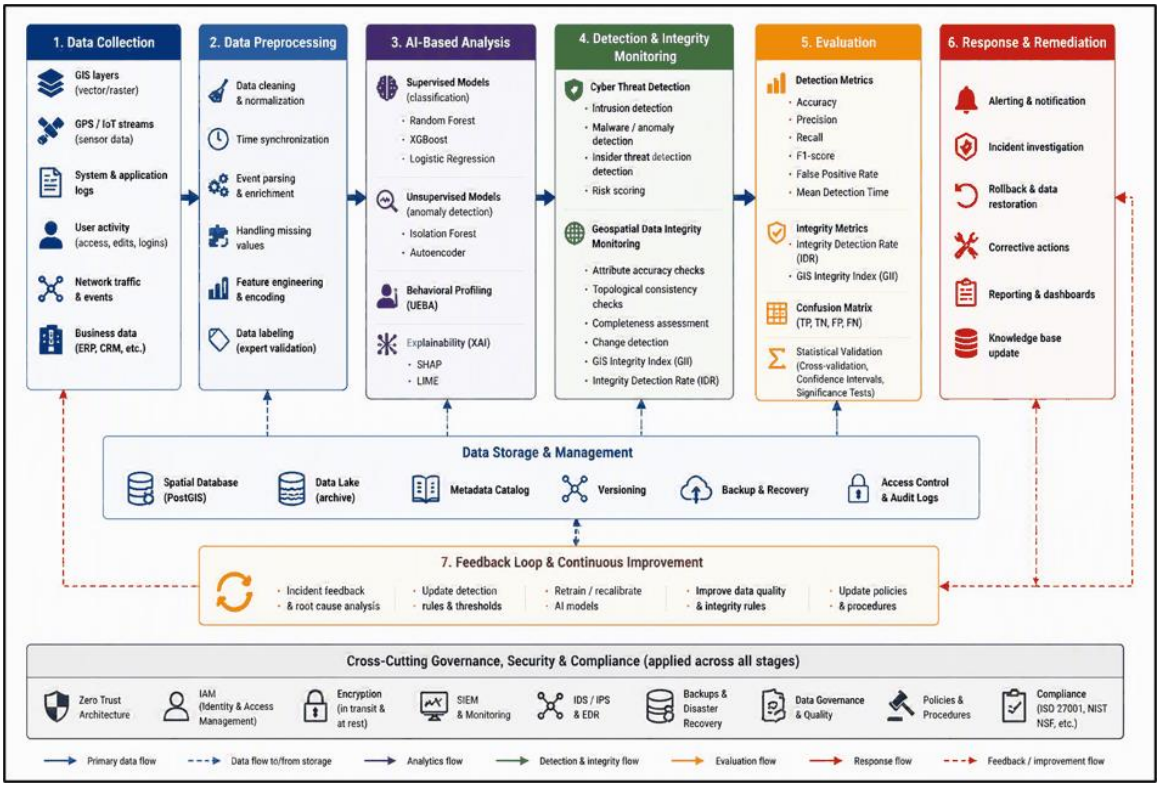

Figure 1. Research model of cyber threat detection and geospatial data integrity protection
Source: own elaboration based on the research model adopted in the case-study protocol; graphic prepared with the support of Microsoft Copilot

The study did not aim to generalize statistically on all GIS enterprises. The results should be interpreted as empirical performance differences observed in the investigated case study. Formal hypothesis testing and confidence intervals were not included, which is treated as a study limitation.

Data preparation, labelling and validation assumptions. The empirical procedure used several categories of input data. Security events and user actions were extracted from SIEM and system logs. GIS database changes were used to identify modifications of object coordinates, attributes and topological relationships. GPS and IoT records were treated as external data streams that could influence spatial analyses. All data categories were time-aligned and normalized before analysis.

Incident labels were assigned through a two-step procedure. First, events were classified automatically according to predefined rule-based criteria and event categories. Second, events relevant to GIS integrity were reviewed by cybersecurity and GIS domain experts. This review was used to confirm whether an event should be treated as a true integrity-related incident, a normal operational change or a false alarm.

The comparison between the traditional and AI-supported systems was based on identical incident categories and the same evaluation logic. The baseline system relied on SIEM correlation rules and known signatures. The AI-supported system used the same baseline data sources, but added classification, anomaly detection and geospatial integrity

monitoring. This design was adopted to make the comparison focused on the added analytical value of AI rather than on differences in data availability. The study did not disclose system-specific product names or sensitive infrastructure details. This was necessary to protect the enterprise investigated. However, the methodological description preserves the logic of the experiment and allows the evaluation framework to be adapted to other GIS environments. The feature groups used by the AI-supported analytical module are listed in Table 6, showing how user, network, GIS, temporal and data-quality variables contributed to the analysis.

Table 6. Feature groups used in the AI-supported analysis

Feature group	Examples	Role in analysis
User activity features	login time, access path, editing frequency	Identification of abnormal user behaviour
Network and system features	source address, event type, SIEM severity	Detection of suspicious security events
GIS change features	coordinate shift, attribute modification, topology change	Assessment of data integrity risk
Temporal features	event sequence, time window, update frequency	Detection of unusual patterns over time
Data quality features	missing values, duplicates, completeness level	GII and anomaly assessment

Source: own elaboration

Case study

Characteristics of the enterprise investigated. The study was conducted in a medium-sized enterprise operating in geoinformation services and spatial analytics. The enterprise collects, processes and analyses geospatial data for planning, infrastructure monitoring, environmental analyses and logistics support. The GIS infrastructure corresponds to modern enterprise GIS architectures described in geoinformation literature (Longley et al., 2015; Duckham et al., 2023).

Geospatial data were used for monitoring technical infrastructure, spatial decision support, operational planning, spatial resource management, reporting and logistics support. From a cybersecurity perspective, the most important threat was unauthorized modification of spatial data leading to unreliable analyses and wrong decisions.

Characteristics of the GIS and AI environment. The enterprise used an integrated GIS environment combining spatial databases, GPS data, IoT measurements, system logs and business application data. GIS data and security events were processed through the GIS platform and SIEM system, while the AI module supported anomaly detection, threat classification and integrity assessment. The solution corresponds to the GeoAI concept, which integrates AI methods and geospatial analysis (Janowicz et al., 2020; Duckham et al., 2023). Because GIS environments increasingly expose geospatial data through web services and APIs, HTTPS/TLS, authentication, authorization and API-level access control should be treated as part of geospatial data integrity protection (Open Geospatial Consortium, 2023). The anonymized GIS-AI-cybersecurity architecture is shown in Figure 2 to clarify the operational environment in which the case-study evaluation was conducted.

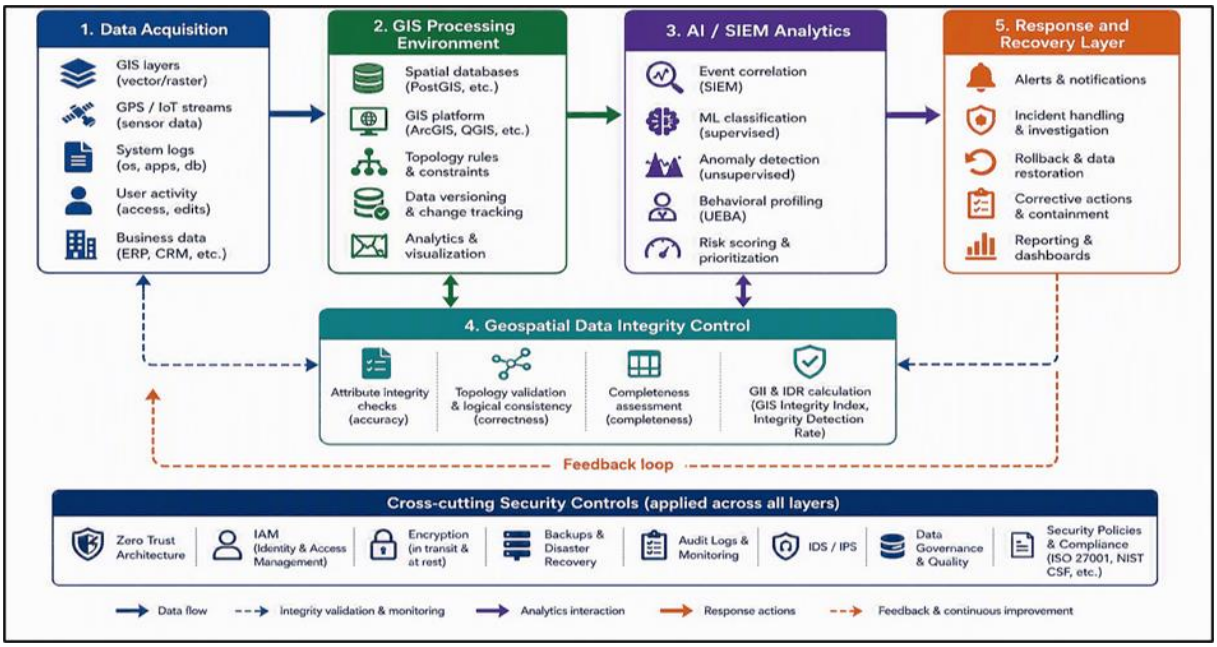

Figure 2. Simplified and anonymized architecture of the GIS-AI-cybersecurity environment considered in the case-study framework
Source: own elaboration based on the anonymized case-study architecture; graphic prepared with the support of Microsoft Copilot

Characteristics of the analyzed cyber threats. The study focused on threats directly affecting geospatial data integrity. Five categories were analysed: unauthorized modification of GIS object coordinates, unauthorized modification of spatial data attributes, violation of topological relationships, GPS and IoT data spoofing, and unauthorized export of geospatial data. These categories were selected because they can affect geometry, attributes, topology, completeness, confidentiality and the operational reliability of spatial analyses.

Implementation of artificial intelligence mechanisms. The AI module was implemented as an extension of the existing cybersecurity architecture. The implementation involved integration of GIS and SIEM data, preparation of historical security events, feature selection, model training, validation and integration with production monitoring procedures. Machine learning was used to identify patterns that were difficult to detect with static rules alone (Buczak & Guven, 2016; Panigrahi et al., 2021).

Research procedure. The implementation procedure included three operational stages. First, the baseline environment using a traditional security system was analysed. Second, the AI module was implemented and configured. Third, the traditional and AI-supported variants were compared using the same categories of incidents, the same evaluation criteria and comparable environmental conditions.

- Stage 1: baseline analysis of the rule-based security system.
- Stage 2: implementation and tuning of the AI module.
- Stage 3: comparative evaluation of detection effectiveness and data integrity protection.

Assumptions for results analysis. The effectiveness of AI implementation was evaluated in two areas: cyber threat detection and geospatial data integrity protection. Support for the hypothesis was assessed through simultaneous improvement in detection indicators, reduction of false alarms, improvement in GII, increase in IDR and reduction of confirmed GIS data anomalies.

Results

Characteristics of identified security incidents. During the observation period, 144 security incidents with potential impact on geospatial data integrity were identified. The most frequent categories were unauthorized modification of spatial attributes and unauthorized modification of GIS object coordinates. Before the incident structure is broken down by threat category, Table 7 explains the relationship between incidents, integrity violations and residual GIS anomalies.

Table 7. Relationship between incident, integrity-violation and anomaly counts

Count	Meaning	Relations to other counts
144 security incidents	Confirmed operational incidents with potential GIS impact	Main incident structure reported by threat category
100 confirmed integrity violations	Standardized subset/test set for IDR evaluation	Used to compare traditional and AI-supported detection of integrity violations
178 GIS anomalies before AI	Record-level anomalies remaining after baseline detection and correction	May include multiple anomalies linked to one incident or operational data-quality issue
25 GIS anomalies after AI	Record-level anomalies remaining after AI-supported detection and correction	Used to show reduction in residual data-integrity problems

Source: own elaboration based on the case-study validation protocol

The numerical categories used in the article refer to different analytical levels. The 144 cases represent confirmed operational security incidents with potential impact on geospatial data integrity. The 100 confirmed integrity violations used for IDR calculation represent a standardized subset of incidents and validation scenarios in which the integrity status could be unequivocally assessed. The 178 and 25 anomaly counts refer to record-level GIS data anomalies remaining after detection and corrective actions. Therefore, several record-level anomalies may be associated with one operational incident or one confirmed integrity violation. The distribution of the identified security incidents by threat category is presented in Table 8, which provides the empirical basis for the subsequent graphical summary.

Table 8. Structure of identified security incidents

Threat category	Number of cases
Unauthorized modification of GIS object coordinates	35
Unauthorized modification of spatial data attributes	42
Violation of topological relationships	21
GPS and IoT data spoofing	17
Unauthorized export of geospatial data	29
Total	144

Source: own elaboration

The incident structure reported in Table 8 is additionally visualized in Figure 3 to make the relative importance of each threat category easier to interpret.

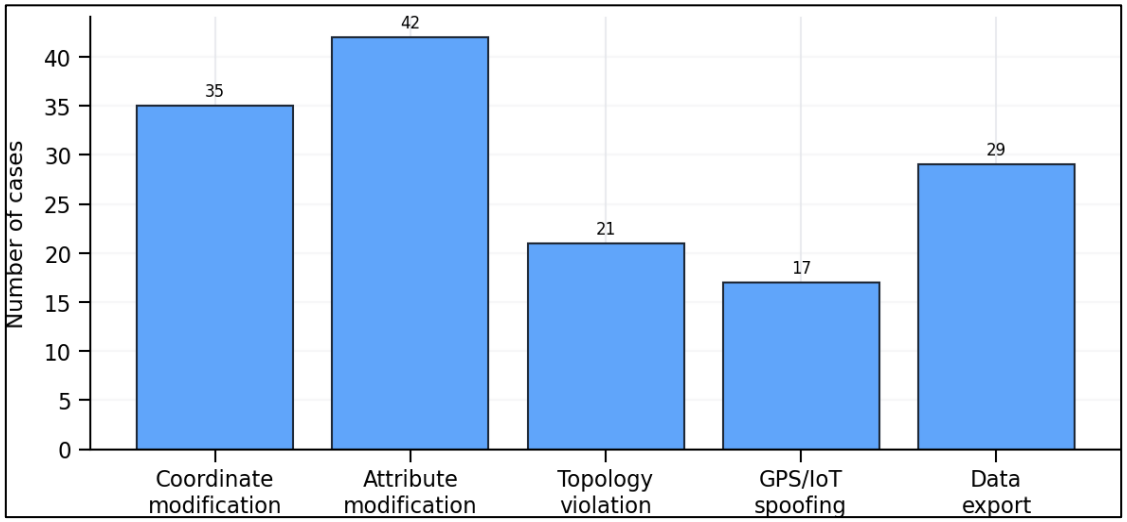

Figure 3. Structure of security incidents identified in the GIS environment
Source: own elaboration

The results show that integrity-related incidents were dominant. Coordinate and attribute modifications accounted for more than half of all analysed cases. This suggests that in GIS environments, data integrity should be treated as a core cybersecurity outcome, not merely as a data quality issue.

Assessment of cyber threat detection effectiveness. The comparison of the traditional and AI-supported systems indicates improvement across all detection indicators. In the validation set with controlled label consistency, Recall increased from 80.1% to 95.5%, which means that the AI-supported system reduced the number of undetected incidents. False Positive Rate decreased from 14.0% to 3.9%, and mean detection time decreased from 14.0 minutes to 2.8 minutes. These values should be interpreted as case-study results based on expert-based validation assumptions adopted within the case-study protocol. The comparative effectiveness of the traditional and AI-supported systems is summarized in Table 9, which reports the main classification and operational detection indicators.

Table 9. Cyber threat detection effectiveness

Indicator	Traditional system	AI-supported system
Accuracy	83.4%	95.8%
Precision	81.4%	94.9%
Recall	80.1%	95.5%
F1-score	80.7%	95.2%
False Positive Rate	14.0%	3.9%
Mean incident detection time	14.0 min	2.8 min

Source: own elaboration

The comparative detection results from Table 9 are presented graphically in Figure 4 to emphasize the differences between the traditional and AI-supported systems.

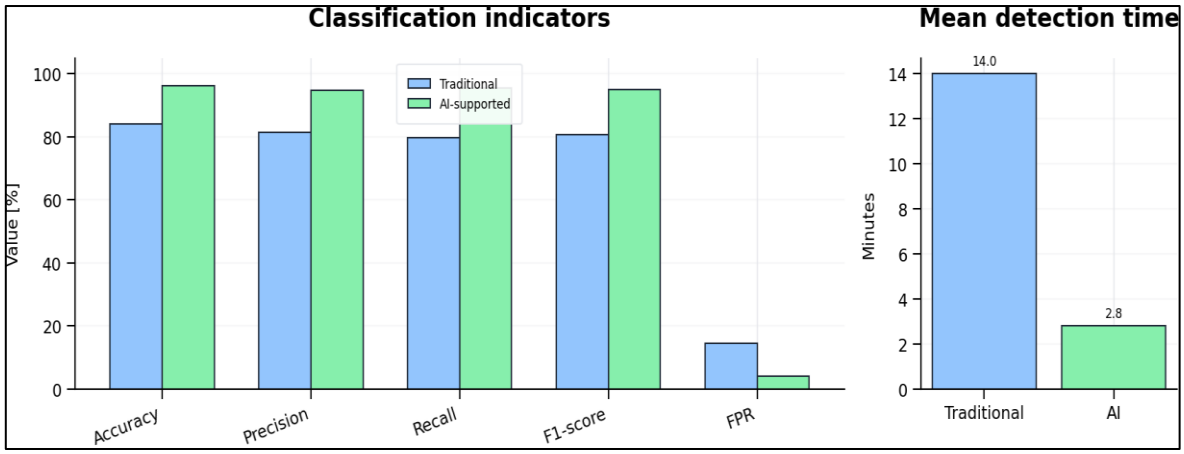

Figure 4. Comparison of cyber threat detection effectiveness and mean detection time.
Source: own elaboration

The improvement should be interpreted within the investigated case study. The strongest operational effect is the combination of higher Recall, lower false alarm rate and shorter detection time. This improves both security effectiveness and the efficiency of the monitoring team.

Impact of artificial intelligence on geospatial data integrity. The GIS Integrity Index increased from 0.91 before AI implementation to 0.98 after AI implementation. The largest improvement concerned logical/topological consistency, which increased from 0.88 to 0.97. This result suggests that AI-supported monitoring was particularly useful for detecting and preventing spatial relationship errors. The effect of AI-supported monitoring on geospatial data integrity is quantified in Table 10 by comparing the GII components before and after implementation.

Table 10. GIS Integrity Index values before and after AI implementation

GII component	Before AI	After AI
Attribute accuracy A	0.91	0.98
Logical/topological consistency T	0.88	0.97
Data completeness C	0.94	0.99
GIS Integrity Index GII	0.91	0.98

Source: own elaboration

The change in the GIS Integrity Index and its components is visualized in Figure 5 to support the interpretation of the before-and-after integrity results.

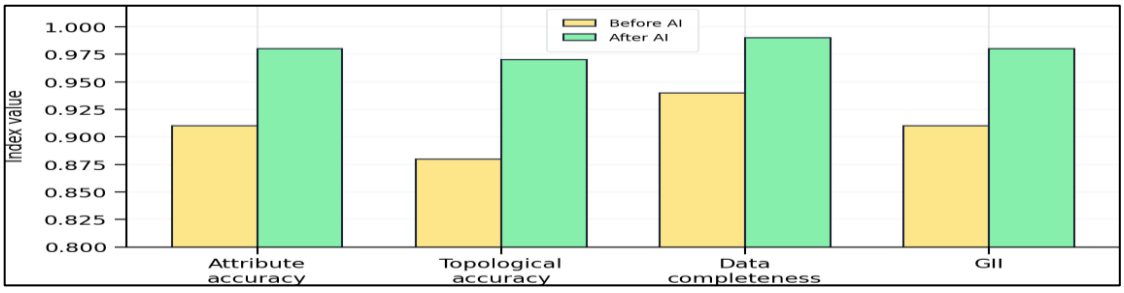

Figure 5. Change in GIS Integrity Index and component values
Source: own elaboration

Analysis of anomaly detection in GIS data. After AI implementation, the number of confirmed GIS data anomalies remaining after detection and corrective actions decreased from 178 to 25. This reduction concerned incorrect coordinates, inconsistent attributes, topology violations, duplicate objects and unauthorized data modifications.

For comparability, the before/after anomaly comparison assumes equivalent six-month observation windows and comparable GIS editing intensity. If the production environment differs across periods, the anomaly counts should also be normalized, for example per 1,000 GIS edits or per month. The detailed reduction of residual GIS data anomalies is shown in Table 11, which separates the before-and-after values by anomaly type.

Table 11. Confirmed GIS data anomalies remaining after detection and corrective actions

Type of anomaly	Before AI	After AI
Incorrect object coordinates	41	7
Inconsistent data attributes	53	9
Topology violations	28	4
Duplicate objects	32	3
Unauthorized data modifications	24	2
Total	178	25

Source: own elaboration

The reduction in confirmed GIS data anomalies is visualized in Figure 6 to complement the detailed anomaly counts reported in Table 11.

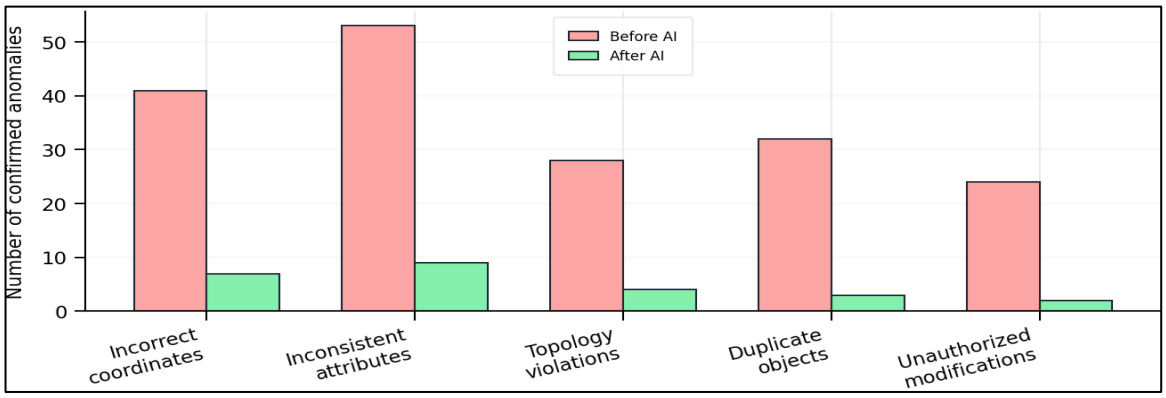

Figure 6. Comparison of confirmed GIS data anomalies before and after AI implementation
Source: own elaboration

The interpretation of this result is not that AI generated fewer alerts, but that AI-supported monitoring and corrective procedures reduced the number of confirmed anomalies remaining in the GIS data environment. This distinction is important for understanding the operational impact of the solution.

Assessment of data integrity violation detection effectiveness. The Integrity Detection Rate increased from 68% in the traditional system to 95% in the AI-supported system. This represents an improvement of 27 percentage points in the detection of confirmed integrity violations. The detection of confirmed data integrity violations is summarized in Table 12, which provides the basis for interpreting the Integrity Detection Rate comparison.

Table 12. Effectiveness of data integrity violation detection

Parameter	Traditional system	AI-supported system
Detected integrity violations	68	95
Confirmed integrity violations	100	100
Integrity Detection Rate IDR	68%	95%

Source: own elaboration

The difference in the Integrity Detection Rate between the traditional and AI-supported systems is shown in Figure 7 to support the interpretation of Table 12.

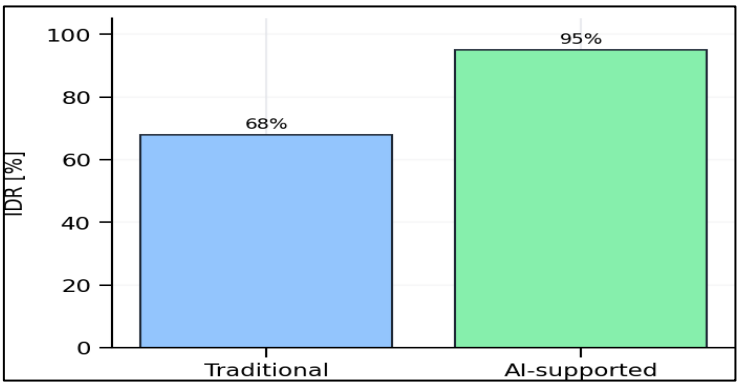

Figure 7. Comparison of integrity detection rate values
Source: own elaboration

Discussion

Interpretation of findings and research hypothesis. The obtained results suggest that AI-supported security monitoring may improve both cyber threat detection and geospatial data integrity protection under the conditions of the investigated enterprise. The results support the research hypothesis within the case-study setting, but they should be interpreted as operational evidence rather than statistically generalisable findings. The relationship between the research hypothesis and the empirical indicators is synthesized in Table 13, linking each hypothesis component with the corresponding result and interpretation.

Table 13. Relationship between research hypothesis components and empirical indicators

Hypothesis component	Indicator	Result	Interpretation
Threat detection effectiveness	Accuracy	83.4% -> 95.8%	Higher classification correctness
Reduction of missed incidents	Recall	80.1% -> 95.5%	Fewer false negatives
Operational efficiency	FPR	14.0% -> 3.9%	Fewer false alarms
Data integrity protection	GII	0.91 -> 0.98	Higher geospatial data quality
Integrity violation detection	IDR	68% -> 95%	Higher detection of manipulation attempts

Source: own elaboration

The main contribution of the study is the integration of cyber threat detection metrics with geospatial integrity indicators. The proposed GIS Integrity Index connects cybersecurity monitoring with GIS data quality assessment. This enables a broader evaluation of AI-supported security mechanisms in GIS environments than a purely network-oriented cybersecurity assessment would provide.

The study also shows that AI does not replace traditional security mechanisms. The most useful approach is complementary: SIEM, rules and access controls provide the baseline, while AI supports adaptive analysis, anomaly detection and data integrity monitoring.

Robustness and interpretation of evaluation results. The numerical improvements observed in the study should be interpreted in relation to the operational context of the enterprise investigated. The AI-supported system improved the detection of incidents affecting geospatial data, but the effect may depend on the maturity of the existing SIEM configuration, the quality of historical data and the stability of normal GIS editing patterns.

The strongest indication of improvement is the simultaneous increase in Recall and decrease in the False Positive Rate. In practical cybersecurity operations, this combination is valuable because it means that fewer incidents remain undetected while the number of unnecessary alerts decreases. In GIS environments this is particularly important because undetected data manipulation can affect subsequent spatial analyses and reports.

The increase in GII should be understood as the effect of enhanced monitoring and corrective procedures rather than as a direct replacement of GIS data governance. AI can identify suspicious modifications and quality anomalies, but procedural validation, access control, versioning and expert review remain necessary. Therefore, the proposed approach should be treated as an extension of geospatial data governance and enterprise security management.

The results also suggest that cybersecurity monitoring in GIS environments should not be limited to infrastructure events. It should include spatial data change monitoring, integrity indicators and anomaly detection applied directly to GIS databases. This integrated perspective is the main methodological value of the proposed approach.

Practical implications of the results. The results suggest that enterprises using GIS should consider AI-supported monitoring as an extension of existing cybersecurity architecture. Practical benefits include faster detection, fewer false alarms, continuous monitoring of geospatial data quality and improved ability to identify subtle modifications of spatial databases. These benefits are especially relevant for sectors such as critical infrastructure, energy, transport, municipal management, crisis management, environmental monitoring, surveying and cartography. Practical implementation should combine AI-supported anomaly detection with incident management procedures, access control, least-privilege principles and continuous verification of trust, especially in GIS environments where data integrity directly affects operational decisions (Kiedrowicz, 2025; Rose et al., 2020).

The practical implications include not only stronger cybersecurity, but also more reliable geospatial decision support. In data-driven enterprises, the integrity of spatial data should be managed jointly by cybersecurity specialists and GIS experts.

Limitations of the study. The study has several limitations. First, it is based on a single case study, which limits the generalisation of the results. Second, the effectiveness of the AI module depends on the quality of training and validation data. Third, the study

focused primarily on integrity, while confidentiality and availability were not analyzed in comparable depth. Fourth, the proposed GII uses expert-defined weights that may require recalibration in other organisations. Finally, formal statistical significance testing was not conducted.

Threats to validity. The main threats to validity concern construct validity, internal validity and external validity. Construct validity is affected by using expert-based validation assumptions for selected quantitative values. Internal validity may be influenced by the configuration of the baseline SIEM rules and by the stability of normal GIS editing patterns during the observation period. External validity is limited because the study is based on a single enterprise environment. These threats were mitigated by using the same event categories, data sources and evaluation logic for both the traditional and AI-supported variants. Nevertheless, further studies should validate the approach across multiple GIS environments and with independently audited operational datasets.

Future research directions. Future research should validate the proposed approach in multiple enterprises and sectors. Further work should also include detailed comparisons of specific AI models, formal statistical testing, sensitivity analysis of GII weights and cross-validation of classification results.

Promising directions include deep learning for geospatial anomaly detection, Explainable Artificial Intelligence for transparent security alerts, integration of GIS with Zero Trust architectures, federated learning for distributed spatial data environments and generative AI for incident reporting and cyber threat analysis (Goodfellow et al., 2016; Rjoub et al., 2023; Rose et al., 2020; Kairouz et al., 2021).

Another limitation concerns the absence of detailed statistical testing. The observed differences are substantial and operationally meaningful, but future studies should include confidence intervals, cross-validation, formal significance testing and sensitivity analysis of GII weights. This would allow stronger conclusions regarding the robustness of AI-supported monitoring.

Future work should also examine model explainability in greater detail. In operational environments, security teams need not only alerts, but also understandable explanations describing why a particular event was classified as suspicious. Explainability is especially important when AI decisions affect spatial data used in infrastructure management, organizational decision-making or crisis management.

Conclusions

The case-study results suggest that artificial intelligence may support both cyber threat detection and geospatial data integrity protection in enterprise GIS environments. Within the adopted case-study validation framework, the AI-supported variant improved classification indicators, reduced false alarms and shortened mean detection time compared with the traditional rule-based system.

The results also indicate a positive relationship between AI-supported monitoring and geospatial data integrity indicators. The GIS Integrity Index increased from 0.91 to 0.98, while the Integrity Detection Rate increased from 68% to 95%. These results should

be interpreted as case-study evidence supported by expert-based validation assumptions rather than as statistically generalisable proof.

The research hypothesis was supported within the investigated case study. The main contribution of the article is the integration of cybersecurity detection metrics with geospatial data integrity indicators, including the proposed GIS Integrity Index. Further research should validate the approach in multiple enterprises, with independently audited datasets, formal statistical testing and sensitivity analysis of the GII weighting scheme.

The findings should be interpreted with caution because of the single-case design and the need for further validation. Nevertheless, the study indicates that AI-supported security architectures may become an important component of modern enterprise GIS environments, particularly where the reliability of spatial data directly affects operational and strategic decisions.

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

Buczak A.L., Guven E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502.

Chandola V., Banerjee A., Kumar V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882.

Duckham M., Sun Q.C., Worboys M. F. (2023). GIS: A Computing Perspective (3rd ed.). CRC Press. https://doi.org/10.1201/9780429168093.

ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [access: 05.07.2026].

Goodfellow I., Bengio Y., Courville, A. (2016). Deep Learning. MIT Press.

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

ISO/IEC (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization.

Janowicz K., Gao S., McKenzie G., Hu Y., Bhaduri B. (2020). GeoAI: Spatially explicit artificial intelligence techniques for geographic knowledge discovery and beyond. International Journal of Geographical Information Science, 34(4), 625–636. https://doi.org/10.1080/13658816.2019.1684500.

Kairouz P., McMahan H.B., Avent B., Bellet A., Bennis M., Bhagoji A.N., Bonawitz K., Charles Z., Cormode G., Cummings R., D'Oliveira R.G.L., Eichner H., El Rouayheb S., Evans D., Gardner J., Garrett Z., Gascon A., Ghazi B., Gibbons P.B., Zhao S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083.

Kiedrowicz M. (2025). GIS security incident management: Practical approaches and standards. GIS Odyssey Journal, 5(1), 59–67. https://doi.org/10.57599/gisoj.2025.5.1.59.

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

NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper, NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29.

Open Geospatial Consortium. (2023). Security and OGC APIs. OGC API Workshop. https://ogcapi-workshop.ogc.org/security/ [access: 05.07.2026].

Panigrahi R., Borah S., Bhoi A.K., Ijaz M.F., Pramanik M., Jhaveri R.H., Chowdhary C.L. (2021). Performance assessment of supervised classifiers for designing intrusion detection systems: A comprehensive review and recommendations for future research. Mathematics, 9(6), 690. https://doi.org/10.3390/math9060690.

Rjoub G., Bentahar J., Abdul Wahab O., Mizouni R., Song A., Cohen R., Otrok H., Mourad A. (2023). A survey on explainable artificial intelligence for cybersecurity. IEEE Transactions on Network and Service Management, 20(4), 5115–5140. https://doi.org/10.1109/TNSM.2023.3282740.

Rose S., Borchert O., Mitchell S., Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800–207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.