GIS Odyssey Journal

2026 • Volume 6 • Number 2

https://doi.org/10.57599/gisoj.2026.6.2.123

Maciej Kiedrowicz[1], Stefan Rozmus[2]

A CASE STUDY ON AI-SUPPORTED DETECTION OF SPATIAL DATA INTEGRITY ATTACKS IN CLOUD-BASED GIS ENVIRONMENTS

Abstract: The development of cloud-based GIS environments has significantly increased the availability, scalability and operational importance of spatial data. At the same time, it has led to the emergence of new challenges in the field of cybersecurity, in particular those related to the protection of the integrity of geospatial resources. Of particular importance are attacks involving unauthorized modification of object geometry, change of descriptive attributes, violation of topological relationships, falsification of location data from GPS systems and IoT devices, as well as unauthorized access to spatial data. The aim of the article is to assess, in an application-oriented case study, the possibility of using artificial intelligence methods to detect attacks violating the integrity of spatial data in cloud GIS environments. The study compares a traditional detection mechanism based on rules and signatures with an AI-supported variant at the system level, rather than providing a full benchmark of individual machine learning algorithms. Three operational indicators were used to assess effectiveness: Attack Detection Effectiveness (ADE), Spatial Data Integrity Impact Index (SDIII) and Attack Response Time (ART). The study analyzed 160 confirmed cases of spatial data integrity violations, including attribute manipulation, coordinate modification, unauthorized data export, topological violations, GPS spoofing, and IoT data manipulation. The results indicate that the AI-assisted system achieved a higher attack detection efficiency than the traditional system. The results obtained indicate that, in the analyzed case study, the use of artificial intelligence methods can significantly increase the effectiveness of protecting the integrity of geospatial data in Cloud GIS environments.

Keywords: artificial intelligence, cloud GIS, cybersecurity, the integrity of spatial data, attack detection

Received: 14 July 2026; accepted: 6 August 2026; revised: 11 August 2026

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

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

Introduction with analysis of the state of the problem

The development of cloud-based geographic information systems has significantly changed the way spatial data is collected, processed, shared and used. Cloud GIS solutions increase the availability, scalability, and operational utility of geospatial services by enabling data to be accessed through web applications, APIs, map services, and distributed data repositories. At the same time, they broaden the surface of a potential attack and increase the importance of protecting the integrity of geospatial resources (Duckham et al., 2023; Open Geospatial Consortium, 2023).

In GIS environments, spatial data integrity is of particular importance because even small modifications to the geometry of objects, annotative attributes, or topological relationships can lead to significant distortion of spatial analysis results. These kinds of breaches may not cause system failures or unavailability of services, but they can result in erroneous maps, incorrect reports, and operational decisions made based on unreliable information (Pascoe et al., 2024; ISO, 2023).

Threats to data integrity in Cloud GIS environments include, m.in, unauthorized modification of object coordinates, manipulation of descriptive attributes, topological violations, GPS spoofing, manipulation of IoT data, API abuse, and unauthorized export of geospatial data. Attacks of this type are particularly problematic because they can be subtle, distributed or gradual, and thus remain beyond the reach of classic security monitoring mechanisms (ENISA, 2024; Open Geospatial Consortium, 2023).

Traditional protection mechanisms, based on rules, signatures and alarm thresholds, remain an important element of the cybersecurity of Cloud GIS environments. However, their effectiveness is limited in the case of unusual, new, or perpetuated events by authorized users or compromised accounts. Security rules can identify known patterns of breaches, but often do not detect minor geometry changes, topological inconsistencies, or unusual sequences of editing operations (Buczak & Guven, 2016; Chandola et al., 2009).

AI can complement classic security by analyzing behavior patterns, classifying security events, detecting anomalies, and identifying unusual changes in spatial data. In the case of Cloud GIS, machine learning methods are of particular importance, as they allow for comparison of current data operations with historical patterns of user activity, attribute changes, geometry modifications, topological rules, and API service behavior (Buczak & Guven, 2016; Janowicz et al., 2020).

To date, research on the use of artificial intelligence in cybersecurity focuses primarily on detecting network intrusions, malware, anomalies in network traffic and protecting cloud infrastructure. On the other hand, research in the field of GIS and GeoAI refers mainly to the analysis of spatial data, image classification, modeling of geographical phenomena and decision support. Relatively less attention is paid to detecting attacks aimed directly at the integrity of spatial data stored and processed in cloud GIS environments (Buczak & Guven, 2016; Janowicz et al., 2020).

The research gap addressed in this article therefore concerns the use of artificial intelligence to detect attacks that target not only the infrastructure of the system, but the geospatial resources themselves. This requires linking cybersecurity signals, such as API

logs and SIEM events, to the spatial and qualitative characteristics of GIS data, including geometry, attributes, topology, and completeness of the data.

The aim of the article is to assess the possibility of using artificial intelligence methods to detect attacks violating the integrity of spatial data in cloud GIS environments. The subject of the analysis is a comparison of the traditional detection mechanism based on rules and signatures with the variant supported by artificial intelligence. The study focuses on attacks affecting object geometry, descriptive attributes, topological relationships, location data, and access to geospatial resources.

The main research question was formulated as follows: how does the use of artificial intelligence methods affect the effectiveness of detecting attacks violating the integrity of spatial data in cloud GIS environments? It was hypothesized that the use of AI methods increases the effectiveness of detecting such attacks compared to traditional security mechanisms based on rules and signatures. The hypothesis was evaluated in a case study using three indicators: Attack Detection Effectiveness (ADE), Spatial Data Integrity Impact Index (SDIII) and Attack Response Time (ART).

The contribution of the article includes three essential elements. First, the need to treat spatial data integrity as a separate cybersecurity goal in Cloud GIS environments was indicated. Second, an approach to assessing the effectiveness of detection based on ADE, SDIII and ART indicators is proposed. Third, an empirical comparison of the traditional variant and the AI-supported variant in a case study of the Cloud GIS environment is presented.

Materials and methods

The aim of the study was to assess the possibility of using artificial intelligence methods to detect attacks violating the integrity of spatial data in cloud GIS environments. The analysis focused on events leading to unauthorized modification of object geometry, changes in descriptive attributes, violations of topological relationships, and interference with the reliability of location data streams from GPS and IoT devices.

The research problem was addressed as a question about how the use of artificial intelligence methods affects the effectiveness of detecting attacks violating the integrity of spatial data in Cloud GIS environments. It hypothesized that the use of AI methods increases the effectiveness of detecting such attacks compared to traditional security mechanisms based on rules, signatures and alarm thresholds. The hypothesis was evaluated in the formula of a case study, so the results obtained should be interpreted as appropriate for the analyzed environment, and not as a basis for statistical generalizations to all cloud GIS systems.

This study should be interpreted as an application-oriented case study conducted in an anonymized operational Cloud GIS environment. It is not intended as a full benchmark of machine learning algorithms. The purpose of the study is to compare two detection variants — a traditional rule-based variant and an AI-supported variant – under the same operational assumptions. Due to security restrictions, detailed logs, user identifiers, infrastructure configuration and complete training datasets are not disclosed.

The subject of the research were the processes of detecting cyberattacks affecting the integrity of spatial data and artificial intelligence mechanisms supporting the identification, classification and assessment of such events. The object of the study was an anonymized Cloud GIS environment used by the company to collect, store, process and share geospatial data. The analyzed environment included a spatial database, geospatial services running in the cloud, APIs, GIS web applications, GPS and IoT data, a security monitoring system, and analytical modules using artificial intelligence methods.

Research material included system and security logs, history of spatial data changes, SIEM events, and location data from GPS systems and IoT devices. The analysis included 160 confirmed cases of events violating the integrity of spatial data. The unit of analysis was a confirmed incident or breach scenario, associated with the attack category, incident source, GIS asset type, detection time, and impact assessment on geometry, descriptive attributes, topology, or data completeness.

The analyzed set of 160 confirmed incidents was collected from operational security monitoring records maintained within the investigated Cloud GIS environment over an extended observation period. Each incident was validated through a multi-stage confirmation procedure combining automated alert correlation, analysis of spatial data modifications, GIS integrity verification procedures, and expert review. Only incidents confirmed simultaneously by technical evidence and expert assessment were included in the final dataset.

For security reasons, the article does not reveal detailed logs, service configurations, user IDs, or infrastructure parameters. Aggregated data were used to evaluate the proposed approach without reproducing sensitive configuration elements of the environment. The validation was comparative: both detection variants were evaluated for the same attack categories, using the same data sources and a uniform incident confirmation procedure. Confirmation of the event included correlation of the technical alert with the analysis of changes in spatial data and expert assessment.

The study used literature analysis, a case study, a comparative analysis and an indicator assessment. The literature analysis made it possible to determine the current state of knowledge regarding the cybersecurity of Cloud GIS environments, the protection of the integrity of spatial data and the use of artificial intelligence in the detection of attacks and anomalies. The case study was used to evaluate the proposed approach in a real-world operating environment, while the benchmarking made it possible to compare the traditional detection mechanism with the AI-supported variant.

The research procedure included the identification of spatial data sources and security events, the acquisition of data from GIS systems, cloud logs, the SIEM system, GPS and IoT streams, and then the cleaning, normalization and temporal synchronization of the data. In the next stage, events that may indicate a breach of spatial data integrity were isolated, the traditional detection mechanism and artificial intelligence models were configured, and then the effectiveness of both approaches was compared using the same attack categories and validation assumptions.

The AI-supported variant used the same data sources, but was expanded to include event classification, anomaly detection, and analysis of user and entity behavior. The

analytical modules were treated as components of the operational detection architecture, while the main objective of the study was to assess the comparative usefulness of the AI-supported variant at the system level. Supervised learning methods, including Random Forest, XGBoost and Multi-Layer Perceptron neural networks, as well as unsupervised methods, including Isolation Forest, Local Outlier Factor and autoencoders, were used as supporting mechanisms for event classification and anomaly detection (Breiman, 2001; Chen & Guestrin, 2016; Buczak & Guven, 2016; Liu et al., 2008; Breunig et al., 2000).

Model development followed a supervised and unsupervised learning workflow. Historical incidents confirmed through the validation procedure were used as labeled examples for classification models, whereas historical operational activity logs were utilized as a baseline for anomaly detection. The objective was not to benchmark individual algorithms but to evaluate the operational effectiveness of an AI-assisted detection architecture at the operational level.

The feature vector included technical, spatial, and behavioral variables. Among others, the type of API operation, the time and sequence of user actions, the scope of object modification, the deviation of coordinates from historical change patterns, the change in the value of critical attributes, the number of topological rule violations, unusual data export patterns, and anomalies in the dynamics of GPS and IoT signals were taken into account. Such a set of features made it possible to link technical cybersecurity signals with the assessment of the quality and consistency of geospatial data.

Validation of the models was carried out in a comparative and scenario mode. Both detection variants were evaluated on the same set of confirmed incidents, while maintaining a uniform procedure for expert confirmation of events. Due to the security limitations of the operating environment, no detailed logs or full error matrices were reported; Therefore, the results obtained should be treated as an application evaluation of a case study, and not as a full statistical experiment.

Standard machine-learning performance measures such as Precision, Recall, F1-score, False Positive Rate, False Negative Rate and PR-AUC were considered during study design. However, complete confusion matrices and event-level datasets could not be disclosed because of operational security restrictions and confidentiality requirements. Consequently, ADE, SDIII and ART were selected as operational indicators enabling a consistent comparison of both detection variants.

The effectiveness of the solution was assessed from three perspectives: the effectiveness of attack detection, the impact of incidents on the integrity of spatial data, and the response time of the system. The basic measure of detection was the Attack Detection Effectiveness (ADE) indicator, which determines the share of detected attacks in the total number of confirmed attacks:

The ADE should be interpreted as a measure of the detectability of confirmed incidents in the analyzed operational environment. It does not replace the full classification score of Precision, Recall, F1-score, False Positive Rate, False Negative Rate or PR-AUC. ADE, SDIII and ART were selected as operational indicators suitable for the anonymized case study and for comparative assessment of two detection variants under identical assumptions.

$$ADE = \frac{N_d}{N_a} \times 100\% \quad (1)$$

where:

N_d – number of detected attacks;

N_a – the total number of confirmed attacks.

The Spatial Data Integrity Impact Index (SDIII) was used to assess the impact of incidents on spatial data quality, which includes four components of data integrity: geometry correctness, attribute correctness, topological compatibility and data completeness:

$$SDIII = \alpha G + \beta A + \gamma T + \delta C \quad (2)$$

assuming:

$$\alpha + \beta + \gamma + \delta = 1 \quad (3)$$

where:

G – Geometry accuracy;

A – Attribute accuracy;

T – topological coherence;

C – Completeness of the data;

α, β, γ, and δ – the weights of the data integrity components.

In this case study, equal weights of SDIII components are assumed, i.e. α = β = γ = δ = 0.25. This assumption was synthetic and comparative. In operational applications, scales should be tailored to the class of data, its criticality, and the importance of individual integrity components in a given decision-making process.

The selection of the four SDIII components was based on commonly recognized GIS data-quality dimensions used in the assessment of geospatial information and aligned with principles reflected in ISO 19157-1:2023. Geometry correctness reflects preservation of spatial object location and shape, attribute correctness reflects preservation of descriptive information, topological coherence reflects preservation of spatial relationships, and data completeness reflects availability of records, layers and metadata. The values of G, A, T and C were normalized to the range from 0 to 1 using expert assessment supported by automated GIS validation procedures.

For the purpose of this case study, the values of G, A, T and C were normalized to the range from 0 to 1, where 1 denotes full preservation of a given integrity component and 0 denotes complete violation of that component. The component values were determined on the basis of expert assessment supported by automated GIS validation procedures, including geometry validation, attribute consistency checks, topology rule verification and completeness assessment of records, layers and metadata. Therefore, SDIII should be interpreted as an operational indicator of preservation of spatial data integrity in the analyzed environment, not as a universally validated metric for all Cloud GIS systems.

The third indicator was Attack Response Time (ART), which determined the average time of detection of an incident violating the integrity of spatial data:

$$ART = \frac{\sum_{i=1}^{n} t_i}{n} \quad (4)$$

where:

t_i – the time of detection of a single attack;

n – The number of incidents detected.

The use of ADE, SDIII and ART indicators enabled a multidimensional assessment of the tested solution. The adopted set of measures allowed to analyze the system not only from the perspective of detection effectiveness, but also in terms of the impact of incidents on the integrity of spatial data and the operational efficiency of the attack detection process.

Case study

The study was conducted in an anonymized enterprise environment using cloud-based GIS solutions to collect, process, analyze and share spatial data. The environment included a spatial database, map services, APIs, GIS web applications, a geospatial data repository, access control mechanisms, a security monitoring system, and data streams from GPS devices and IoT sensors.

The spatial data resources used in the studied environment included vector layers, attribute data, GPS location data, measurement data from IoT devices, and metadata. The key factors were those categories of data whose modification could directly affect the results of GIS analyses: object geometry, descriptive attributes, topological relationships and completeness of data sets.

Spatial data integrity was understood as maintaining the correctness of geometry, reliability of descriptive attributes, topological consistency and completeness of data. Operationally, component G stood for geometry correctness, component A for attribute correctness, component T for topological compatibility, and component C for completeness of records, layers, and metadata necessary to perform spatial analysis.

The case study analysed six categories of attacks on spatial data integrity: geometry manipulation, attribute manipulation, topological violations, GPS spoofing, IoT data manipulation, and unauthorized access or export of spatial data. Manipulations of geometry, attributes, and topology can directly alter the position, description, or spatial relationships of GIS objects, leading to erroneous analyses even if there is no system failure. On the other hand, GPS spoofing, IoT data manipulation and unauthorized data export can affect the reliability of location streams or be a preparatory stage for subsequent attacks on GIS assets.

AI engines were used as an extension of traditional rule-based security monitoring, access control, threshold alerts, and SIEM. The AI variant included event classification, anomaly detection, and analysis of user and entity behavior. The logical architecture of the AI-supported variant is presented in Figure 1 as a sequence including GIS and security data sources, data normalization and temporal synchronization, extraction of spatial, behavioral and technical features, application of anomaly classification and detection models, risk scoring, correlation with the SIEM system, and analytical decision and launch of data integrity restoration procedures.

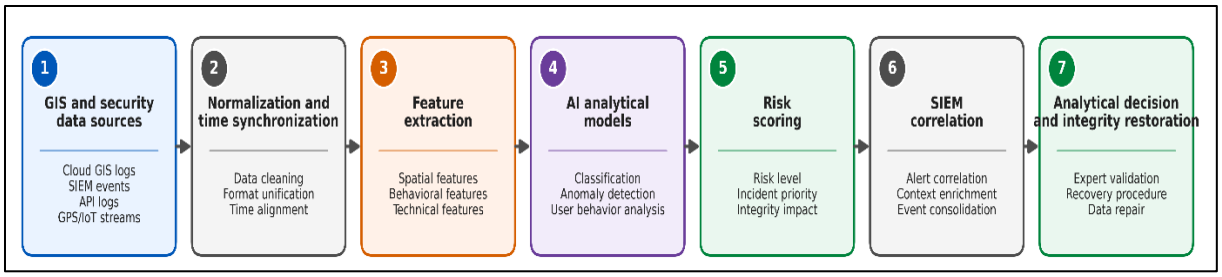

Figure 1. Logical architecture of an AI-enabled detection variant in a GIS cloud environment
Source: own development

Results

In the examined Cloud GIS environment, 160 confirmed cases of events violating the integrity of spatial data were identified. The analysis was mainly focused on attacks aimed at unauthorized modification of object geometry, manipulation of descriptive attributes, violations of topological relationships, falsification of location data and unauthorized access to geospatial resources. The structure of the identified incidents is presented in Table 1.

Table 1. Structure of identified attacks on spatial data integrity

Attack category	Number of cases	Total share
Manipulating Attributes	42	26.3%
Coordinate manipulation	36	22.5%
Unauthorized export of spatial data	28	17.5%
Topology violation	22	13.8%
GPS spoofing	17	10.6%
IoT Data Manipulation	15	9.3%
Total	160	100.0%

Source: own development

The structure of the identified attacks is also presented in Figure 2.

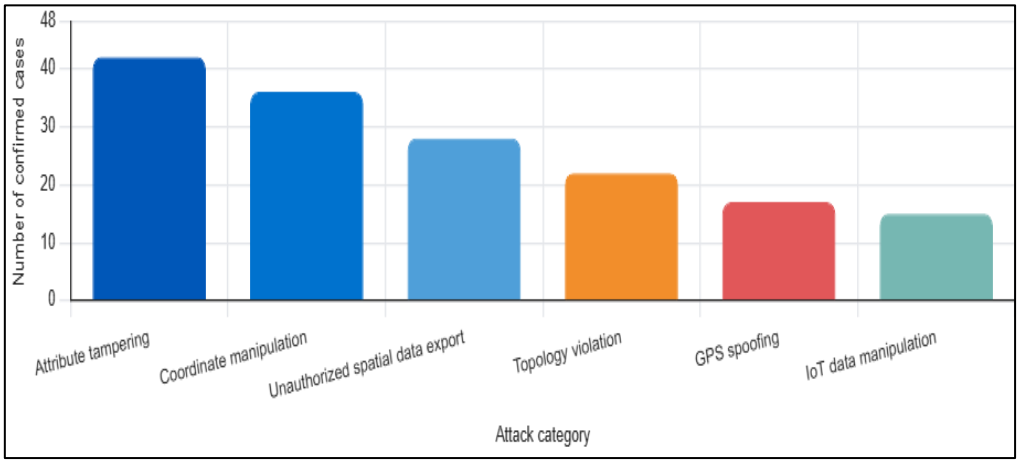

Figure 2. Structure of identified attacks on spatial data integrity
Source: own development

The results indicate that the most common attacks were those involving the manipulation of descriptive attributes and the modification of the coordinates of spatial objects. These categories accounted for a total of 48.8% of all analyzed cases. This means that in the studied Cloud GIS environment, threats to the integrity of spatial data most often concerned direct interference with the descriptive or geometric properties of GIS objects. On the other hand, the significant share of unauthorised export of spatial data indicates that incidents traditionally classified as confidentiality breaches may also support subsequent actions aimed at manipulating geospatial resources.

To assess the effectiveness of detection, a traditional system based on rules, signatures and alarm thresholds was compared with an AI-powered solution. The comparison was carried out for the same attack categories and using uniform validation assumptions. The results are presented in Table 2.

Table 2. Effectiveness of detection of attacks on the integrity of spatial data

Attack category	Traditional system	A system based on artificial intelligence
Coordinate manipulation	71%	94%
Manipulating Attributes	75%	96%
Topology violation	69%	92%
GPS spoofing	78%	97%
IoT Data Manipulation	74%	95%
Unauthorized export of spatial data	82%	98%
Average ADE	74.8%	95.3%

Source: own development

Figure 3 shows a comparison of the detection effectiveness of individual attack categories.

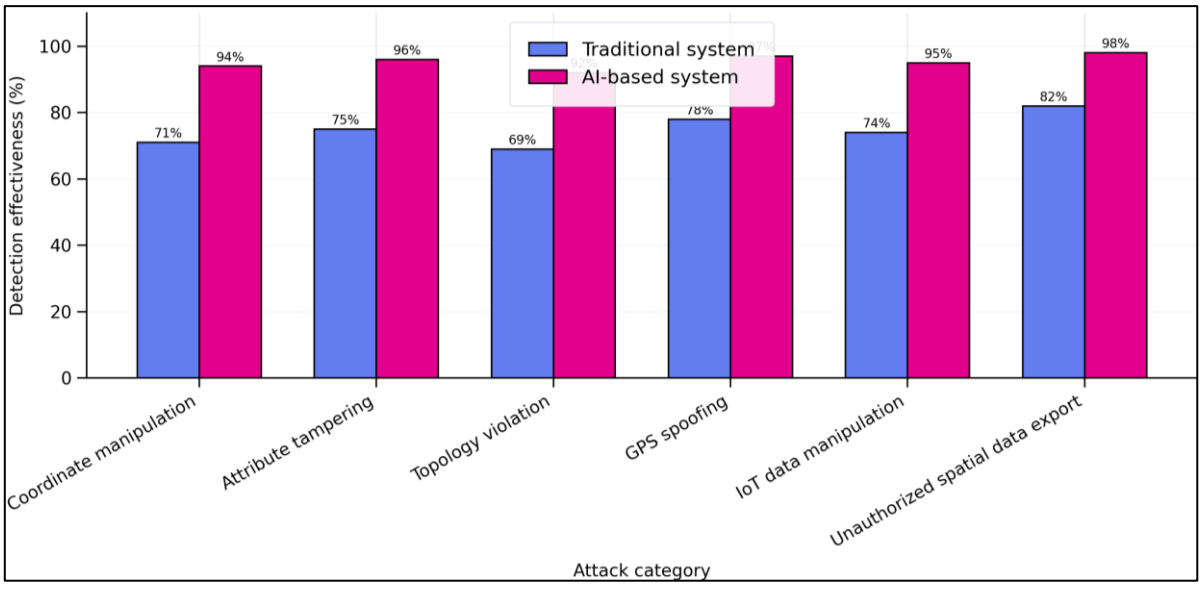

Figure 3. Effectiveness of detection of attacks on the integrity of spatial data
Source: own development

In each of the analyzed categories, the AI-supported variant achieved higher detection efficiency than the traditional system. The average value of the Attack Detection Effectiveness indicator increased from 74.8% to 95.3%, which means an improvement of 20.5 percentage points. Improving the detection of topological breaches and manipulation of IoT data is of the greatest practical importance, as these types of events are often subtle, distributed or dependent on the operational context. The AI variant also better identified cases of GPS spoofing and unauthorized data export, which confirms the usefulness of classification, anomaly detection, and event correlation mechanisms in Cloud GIS environments.

The Spatial Data Integrity Impact Index was used to assess the impact of detected incidents on the quality of spatial data. It takes into account four components of data integrity: geometry correctness, attribute correctness, topological compatibility, and data completeness. The results are presented in Table 3.

The designations "Before AI" and "After AI" should be understood as a comparison of the non-AI-assisted detection variant and the AI-enhanced variant, rather than as a full longitudinal before-after experiment in the statistical sense.

Table 3. Spatial data integrity impact index before and after AI implementation

SDIII Components	Before AI	AI-supported variant
G Geometry Accuracy	0.87	0.97
Attribute A accuracy	0.89	0.98
Topological Coherence T	0.84	0.96
Data completeness C	0.92	0.99
SDIII	0.88	0.98

Source: own development

The change in the value of the SDIII indicator and its components is shown in Figure 4.

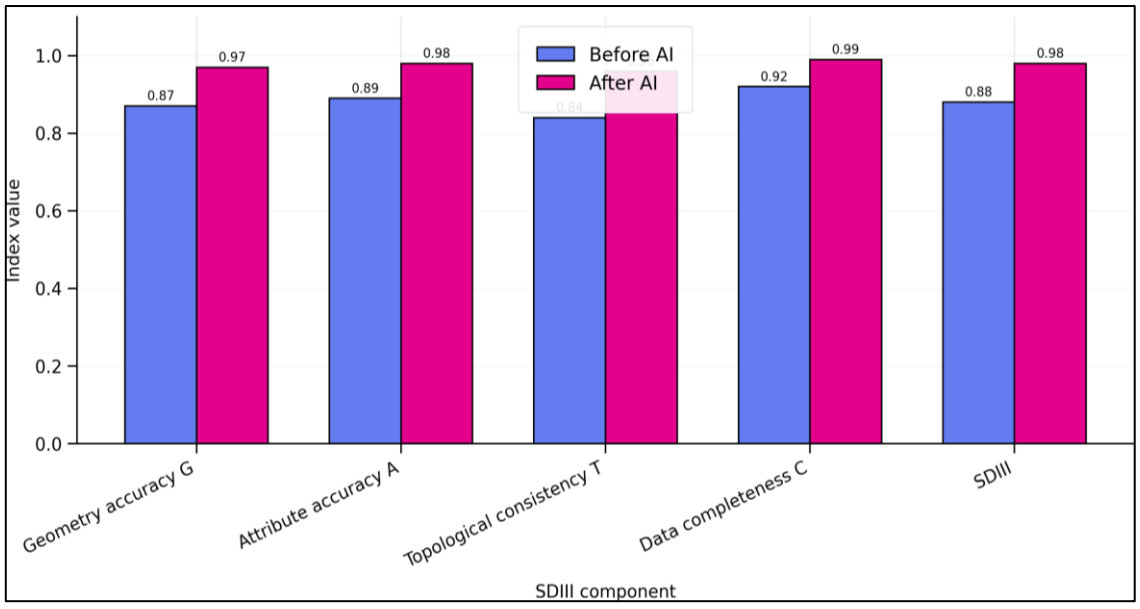

Figure 4. Change in the Spatial Data Integrity Impact Index and its components
Source: own development

The value of the synthetic SDIII index increased from 0.88 to 0.98, which indicates a reduction in the negative impact of incidents on the quality of geospatial data after the use of artificial intelligence mechanisms. The greatest improvements were noted in topological compatibility and geometry correctness. This result suggests that AI methods are particularly useful in detecting anomalous spatial changes, such as network continuity violations, invalid object intersections, neighborhood relationship changes, or unauthorized geometry shifts. The improvement in attribute components and data completeness further indicates that AI can support the detection of manipulation of descriptive values and events that affect the completeness of GIS assets.

Another element of the assessment was the average attack detection time, determined by the Attack Response Time indicator. In Cloud GIS environments, detection time is important because manipulated data can be quickly used by multiple users, web applications, APIs, and automated analytics services. The results of the comparison are presented in Table 4.

Table 4. Attack response time by attack category

Attack category	**Traditional system**	**A system based on artificial intelligence**
Coordinate manipulation	15.4 min	3.6 min
Manipulating Attributes	12.8 min	2.9 min
Topology violation	14.7 min	3.4 min
GPS spoofing	11.6 min	2.5 min
IoT Data Manipulation	13.2 min	3.1 min
Unauthorized export of spatial data	10.4 min	2.3 min
Average ART	13.0 min	3.0 min

Source: own development

Figure 5 shows a comparison of the response time of the system for individual attack categories.

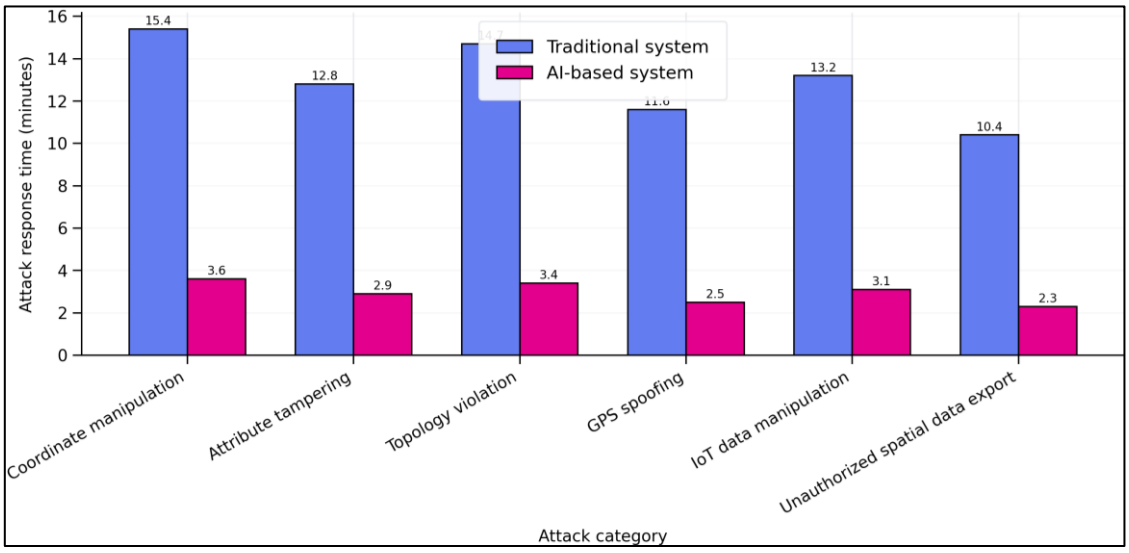

Figure 5. Attack response time by attack category
Source: own development

The AI-powered system reduced the average detection time in all the categories analysed. The average ART decreased from 13.0 minutes in the traditional system to 3.0 minutes in the AI variant. This means a reduction in the average detection time by 10.0 minutes. Reducing detection time for coordinate manipulation, topological violations, and IoT data manipulation is of paramount operational importance, as these events can quickly impact spatial analysis, reporting, and ongoing monitoring of field objects. A synthetic comparison of the three main assessment indicators is presented in Table 5.

Table 5. A high-level comparison of traditional and AI-based detection

Indicator	Traditional system	A system based on artificial intelligence
ADE	74.8%	95.3%
SDIII	0.88	0.98
ART	13.0 min	3.0 min

Source: own development

Discussion

The compilation of results shows a clear advantage of the AI-enabled variant in the analyzed case study and under the adopted validation assumptions. The AI system achieved higher attack detection efficiency, reduced the impact of incidents on the integrity of spatial data, and significantly reduced the time of threat identification. The most important practical benefit is the combination of high detection with faster response times. In Cloud GIS environments where the same spatial data is used in parallel by users, web applications, APIs, and analytics services, rapid detection limits the period of time that manipulated data can remain active in the system.

When interpreting the advantage of an AI variant, it is necessary to take into account the configuration of the traditional system, the quality of the input data, and the range of attack scenarios adopted. The results show the advantage of the AI approach in the analyzed environment and with the adopted validation assumptions, but they do not determine the same level of improvement in each Cloud GIS architecture.

The results confirm that protecting cloud-based GIS environments should not be limited to infrastructure security, access control, and technical event monitoring. In the case of GIS systems, it is equally important to protect the quality, consistency and reliability of the spatial data itself. Violation of the integrity of geometry, attributes, topologies, or location streams may not cause system failure, but it can lead to erroneous analyses, incorrect reports, and decisions based on distorted information.

The results also indicate that a hybrid approach is the most justified. Rule-based mechanisms, access control, API monitoring, and SIEM remain essential for detecting known threat patterns and enforcing security policies. Artificial intelligence, on the other hand, acts as an adaptive layer, capable of detecting anomalies, unusual data changes, and deviations from standard patterns of user and service activity. In such a model, AI does not replace classic security, but increases the system's ability to detect attacks aimed directly at the integrity of geospatial assets.

It should be emphasized that the presented results are of an applicative nature and refer to the analyzed case study. They do not constitute the basis for full statistical generalization to all cloud GIS environments. However, the consistent advantage of the AI variant in all major indicators indicates the high usefulness of this approach and justifies further research into intelligent mechanisms for protecting the integrity of spatial data in Cloud GIS environments.

Implications, limitations, and future directions of research. The practical implication of the results is that the use of AI methods can significantly strengthen the protection of spatial data integrity in Cloud GIS environments. In particular, AI can accelerate the identification of unauthorized changes to geometry, descriptive attributes, topological relationships, and location data streams. This is important in environments where the same geospatial resources are used simultaneously by multiple users, web applications, APIs, and automated analytics services.

The implementation of AI mechanisms can support the automatic detection of unusual data changes, the analysis of anomalies in user and service activity, the reduction of attack detection time, the prioritization of incidents according to their impact on data integrity, the audit of changes in GIS resources, and increasing the reliability of spatial analyses. However, the greatest practical value is not the use of AI as a separate module, but its integration with existing security mechanisms, such as access control, API monitoring, SIEM system, data versioning and procedures for restoring correct versions of spatial resources.

The results of the survey also indicate the need for closer cooperation between cybersecurity specialists, administrators of cloud environments and GIS experts. Attacks on the integrity of spatial data are interdisciplinary in nature, as their effects concern information security, the quality of geospatial data and the reliability of decision-making processes at the same time. Effective protection of Cloud GIS environments therefore requires a combination of technical, spatial and analytical competencies.

The limitations of the study result primarily from the adopted formula of a single case study, the aggregated nature of the data, and the dependence of the effectiveness of AI models on the quality of input data, the correctness of event labeling and the representativeness of the analyzed attack scenarios. Due to the security of the investigated environment, detailed logs, system configurations or user IDs were not disclosed. This limits the ability to fully replicate the study, but at the same time protects sensitive information about the infrastructure and organization of security processes.

An important limitation is also the ability to change user behavior patterns, API services, and data streams over time. This phenomenon can affect the effectiveness of detection models and requires periodic recalibration, updating of behavioral profiles, and monitoring of the number of false alarms. In practical implementations, it is therefore necessary to treat AI models as elements of a dynamic security system, and not as a static detection mechanism.

The main risks to the accuracy of results relate to how data integrity components are defined and weighted, the configuration of the underlying system, the quality of labels, and the limited external relevance resulting from the analysis of a single Cloud GIS

environment. In other organizational environments, the meaning of individual integrity components, such as geometry, attributes, topology, and data completeness, may be different. Therefore, the proposed ADE, SDIII, and ART indicators should be further validated across different data classes, access models, and cloud architectures.

Further research should include validation of the proposed approach in multicloud, hybrid, and distributed environments. It is particularly important to test the effectiveness of AI models in systems with different processing scales, different user profiles and different types of spatial data, such as transport networks, technical infrastructure, administrative layers, GPS/IoT dynamic data and surface objects.

Another direction of research should be the development of methods of explainable artificial intelligence. In the context of GIS cybersecurity, it is important not only to generate an alert, but also to indicate why a given change in geometry, attribute, topological relationship or access pattern was considered suspicious. Model explainability can increase analyst confidence, facilitate incident auditing, and foster collaboration between security teams and GIS experts (Rjoub et al., 2023).

You can also develop federated learning-based approaches that can enable you to train detection models on data from multiple enterprises or organizations without having to centrally share sensitive geospatial resources. This approach can increase the resilience and effectiveness of models, while maintaining confidentiality, data protection, and organizational security requirements (Kairouz et al., 2021).

In future research, it is also reasonable to take into account the resistance of AI models to adversary attacks and the risk of poisoning training data. A potential attacker may try to modify the data in a way that makes it difficult to detect anomalies or affect the data used to train models. Therefore, it is necessary to test the resilience of models against detection bypass scenarios, intentional interference and manipulation of training sets.

Ultimately, further work should be aimed at integrating AI-enabled detection with Zero Trust architecture, identity management, API access control, data versioning, change auditing, and automatic procedures for restoring correct versions of spatial assets. This approach will move from incident detection alone to a full lifecycle of protecting the integrity of spatial data in Cloud GIS environments (Rose et al., 2020; Open Geospatial Consortium, 2023).

Conclusion

The study indicates that artificial intelligence methods can significantly support the detection of attacks violating the integrity of spatial data in cloud GIS environments. Compared to the traditional approach based on rules, signatures, and alarm thresholds, the AI-enabled variant demonstrated greater efficiency in identifying events related to manipulation of geometry, descriptive attributes, topological relationships, GPS/IoT data, and access to geospatial resources.

The results of the case study confirm the superiority of the AI variant in three dimensions of the assessment. The average attack detection efficiency, expressed by the Attack Detection Effectiveness (ADE) indicator, increased from 74.8% for a traditional system to 95.3% for an AI-powered system. At the same time, the Spatial Data Integrity

Impact Index (SDIII) increased from 0.88 to 0.98, indicating a reduction in the negative impact of incidents on the quality and reliability of spatial data. Significant improvements were also noted in response time, with the average Attack Response Time (ART) reduced from 13.0 minutes to 3.0 minutes.

The most important conclusion from the study is the need to treat spatial data integrity as a self-contained cybersecurity goal in Cloud GIS environments. Protecting these types of systems should not be limited to securing infrastructure, network services, APIs, and access control mechanisms. It is equally important to continuously monitor the quality, consistency and reliability of the geospatial resources themselves, as even small modifications to geometry, attributes or topology can lead to erroneous spatial analyses and incorrect operational decisions.

The adopted research hypothesis was supported by the analyzed case study. This means that, in the examined Cloud GIS environment and under the adopted operational assumptions, the use of AI methods increased the effectiveness of detecting attacks on the integrity of spatial data compared to traditional security mechanisms. However, the results are of an applicative nature and refer to the studied environment, so they should not be treated as a basis for full statistical generalization for all cloud-based GIS systems or as a complete benchmark of individual machine learning algorithms.

The contribution of the article includes three essential elements. Firstly, the need to consider the integrity of spatial data as a separate and important area of cybersecurity was indicated. Secondly, a model for assessing the effectiveness of detection based on ADE, SDIII and ART indicators was proposed, combining a technical perspective with an assessment of the quality of geospatial data. Third, an empirical comparison of a traditional system and an AI-enabled system in a real-world Cloud GIS case study is presented.

Artificial intelligence should not be treated as a substitute for classic security mechanisms, but as a complement to them. The hybrid approach has the greatest practical value, in which AI supports SIEM systems, API monitoring, access control, change auditing, data versioning, and procedures for restoring correct GIS resources. In such a model, AI acts as an adaptive analytical layer, increasing the system's ability to detect subtle, unusual or gradual violations of the integrity of spatial data.

Future research should extend the evaluation framework by incorporating Precision, Recall, F1-score, False Positive Rate, False Negative Rate, ROC analysis and PR-AUC metrics. Broader validation across different Cloud GIS environments, spatial-data classes and cloud architectures would further improve transparency, reproducibility and comparability of results while supporting assessment of model robustness against adversarial attacks, poisoning and concept drift.

It will be particularly important to expand the assessment to include standard machine learning evaluation measures such as Precision, Recall, F1-score, False Positive Rate, False Negative Rate and PR-AUC, as well as to analyze the resistance of AI models to adversarial attacks and poisoning of training data. The integration of AI-assisted detection with Zero Trust architecture, explainable artificial intelligence, federated learning, and

procedures for automatic restoration of correct versions of spatial data also remains an important direction.

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

Breiman L. (2001). Random forests. Machine Learning, 45(1), 5–32. https://doi.org/10.1023/A:1010933404324.

Breunig M.M., Kriegel H.P., Ng R.T., Sander J. (2000). LOF: Identification of local deviations based on density. In the proceedings of the ACM SIGMOD 2000 International Conference on Data Management, pp. 93–104. ACM. https://doi.org/10.1145/335191.335388.

Buczak A.L., Guven E. (2016). An overview of data mining and machine learning methods for detecting cybersecurity intrusions. 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: Overview. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882.

Chen T., Guestrin C. (2016). XGBoost: Scalable tree reinforcement system. In: 22. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785–794. ACM. https://doi.org/10.1145/2939672.2939785.

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

ENISA (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://data.europa.eu/doi/10.2824/0710888.

ISO (2023). ISO 19157-1:2023 Geographic Information – Data Quality – Part 1: General Requirements. International Organization for Standardization.

Janowicz K., Gao S., McKenzie G., Hu Y., Bhaduri, B. (2020). GeoAI: Spatially distinct AI techniques for discovering geographic knowledge 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., Gascón A., Ghazi B., Gibbons P.B. (2021). Progress and open problems in federation learning. Fundamentals and Trends in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083.

Liu F.T., Ting K.M., Zhou Z.H. (2008). Isolation forest. In: 8. IEEE International Conference on Data Mining, pp. 413–422. IEEE. https://doi.org/10.1109/ICDM.2008.17.

Open Geospatial Consortium (2023). OGC Security and API. API OGC workshop. https://ogcapi-workshop.ogc.org/security/.

Pascoe C., Quinn S., Scarfone K. (2024). NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper, NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.

Rjoub G., Bentahar J., Abdul Wahab O., Mizouni R., Song A., Cohen R., Child H., Mourad A. (2023). Survey on explainable AI 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.