GIS Odyssey Journal

2025 • Volume 5 • Number 2

https://doi.org/10.57599/gisoj.2025.5.2.151

Jerzy Stanik[1], Maciej Kiedrowicz[2]

CLOUD DATA SECURITY: PRACTICES AND STANDARDS FOR GIS

Abstract: In the era of growing popularity of cloud computing, ensuring data security in GIS (Geographic Information Systems) systems is becoming a key challenge. The purpose of this article is to analyze cloud data security practices and standards that can be used in GIS systems. The study used hazard and risk analysis methods, a literature review, interviews with experts and a case study. The results indicate that the most common threats to GIS data in the cloud include unauthorized access, ransomware attacks, and human error. Effective security practices include the use of advanced monitoring tools, data encryption, and the implementation of international standards such as ISO 27001, ISO 27017, and ISO 27018. The article concludes with recommendations for improving data security in the cloud and proposals for further research in this area.

Keywords: Data security, Cloud computing, GIS systems, ISO standards, Risk management

Received: 19 May 2025; accepted: 27 August 2025

[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/0000-0002-4389-0774; email: maciej.kiedrowicz@wat.edu.pl

Introduction

Cloud computing has become an integral part of modern information systems, including geographic information systems (GIS). The use of cloud computing in GIS makes it possible to store, process and analyze huge amounts of spatial data in a more efficient and scalable way (USC GIS Graduate Programs, 2021). With cloud computing, GIS users can access data and analytics from anywhere, anytime, dramatically increasing their productivity and collaboration capabilities (Spatial Post, 2021). However, with the growing importance of cloud computing, there are also challenges related to data security. Storing GIS data in the cloud exposes it to a variety of threats, such as unauthorized access, ransomware attacks, and human error (Ellipsis Drive). Spatial data is often sensitive and critical to the functioning of many organizations, so its protection is crucial (Ndamukunda, 2024). Therefore, it is crucial to ensure that appropriate security measures are in place to protect your data from loss, theft, or damage. The use of cloud computing in GIS brings numerous benefits, such as scalability, flexibility, availability and reduction of infrastructure costs (GIS Cloud, 2017). Despite the growing body of research on cloud data security, the specific risks to GIS data and the effectiveness of various security practices are relatively poorly studied. There is a need for more detailed research into how GIS data is protected in the cloud, including the effectiveness of encryption, authentication, monitoring, and compliance with international standards. Investigating these vulnerabilities is important for improving the security of data in GIS systems and minimizing the risks associated with data storage and cloud processing.

The main research concern is to ensure the security of GIS data in the cloud while maintaining its availability and integrity. In particular, the study focuses on analyzing cloud data security risks, practices, and standards in the context of GIS. Research questions include:

- What are the most common threats to GIS data security in the cloud?
- What practices and technologies are most effective in ensuring the security of GIS data in the cloud?
- To what extent are international standards such as ISO 27001, ISO 27017, ISO 27018 applied in the context of GIS data security in the cloud?
- What are the main challenges of implementing cloud data security standards for GIS?

The purpose of this article is to analyze cloud data security practices and standards that can be used in GIS systems. The article aims to identify the most common threats to GIS data in the cloud and to assess the effectiveness of various security practices and technologies. In addition, the article analyzes compliance with international security standards such as ISO 27001, ISO 27017, and ISO 27018, and discusses the challenges of implementing these standards in the context of GIS. There are many studies and publications on data security in the cloud, but specific aspects related to GIS are relatively rarely discussed. The research focuses mainly on the general principles of cloud data security, such as encryption, authentication, and monitoring (Ellipsis Drive) In the context of GIS, it is important to take into account the specific challenges related to spatial data

and interoperability of systems. A literature review points to the need for more detailed research on the risks and practices of GIS data security in the cloud (Young, 2013).

The article begins with an introduction that discusses the background, research gap, research problem, and research questions that focus on ensuring the security of GIS data in the cloud while maintaining its core security attributes (confidentiality, availability, and integrity). The next chapter is methodology, which describes the research methods and data sources used in the analysis. The Results chapter contains a description of the process of implementing data security in the cloud, with particular emphasis on the importance of the process of identifying the most common threats and risk assessment. It also covers the main challenges related to cloud security, key elements of cloud security, best practices for securing data in the cloud, tools and technologies supporting cloud security, the role of encryption in data protection in cloud environments, identity and access management in the cloud, security monitoring and auditing in cloud environments, regulatory compliance and security in the cloud. These results are also discussed in the context of the existing literature. The conclusions and recommendations summarize the main results and propose practical recommendations and directions for future research.

Methodology

A variety of research methods have been used to analyze the security of cloud data for GIS systems. A detailed literature analysis was conducted to identify existing risks and security practices. Qualitative methods such as interviews with data security and GIS experts were also used to gain deeper insight into specific challenges and solutions. In addition, quantitative methods, including surveys for GIS users, were used to collect data on their experiences and practices related to data security in the cloud. Risk analysis was performed using risk assessment tools that identified and classified hazards and assessed their potential impact on GIS systems.

In addition, a thematic analysis method was used to identify and analyse the main themes and patterns in the collected qualitative data. The thematic analysis made it possible to isolate key threats and security practices that appeared in interviews and surveys, allowing for a better understanding of cloud data security issues for GIS systems.

The study used a variety of data sources to provide a comprehensive analysis. The main data sources included security incident reports, which provided information on real-world cloud data breaches. Surveys of GIS users provided data on their experiences and security practices. Interviews with experts in the field of data security and GIS provided detailed information on specific challenges and effective solutions. In addition, a review of the scientific and industry literature provided theoretical context and allowed for the identification of research gaps and existing cloud data security practices and standards.

The study also included a review of currently available domain and specialist reports on the global market. These reports provided valuable insights into the latest trends, challenges, and best practices in cloud data security. Examples of such reports include the "2022 Cloud Security Report" prepared by Check Point Software, which analyzes cloud

data security incidents, and "Cloud Data Security in 2025" (Markiewicz, 2025; Orca Security, 2022). A review of these reports allowed us to obtain up-to-date data and conclusions that were included in the analysis.

Results

The process of implementing data security in the cloud. The process of implementing data security in the cloud includes several key steps that help ensure that data is protected against a variety of threats (Fig. 1.). Implementing these steps helps you create a comprehensive cloud data security strategy that protects against a variety of threats and ensures regulatory compliance.

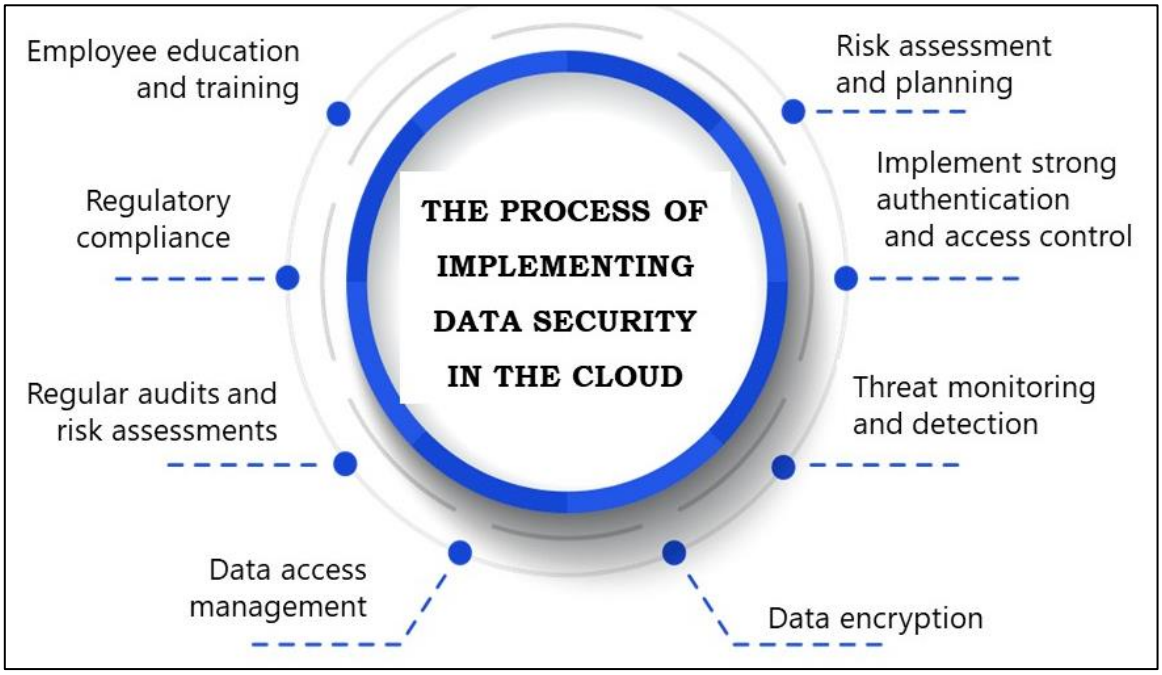

Fig. 1. Stages of implementation of data security in the cloud
Source: own study

The first step is to conduct a risk assessment to identify potential threats and weaknesses in the system. Based on the results of the assessment, a security plan is created that sets out data protection measures and procedures. Implement strong authentication and access control: Implementing authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC) is crucial. A Zero Trust approach, which assumes that no person or device is automatically trusted, also helps to secure data. The second step is to encrypt your data both in transit and at rest. End-to-end encryption ensures that data is protected at every stage of its lifecycle. Regular monitoring of cloud systems allows you to quickly detect and respond to potential threats. Threat intelligence tools and security incident and event management (SIEM) systems are very helpful here. Managing access to data is an important step. It's important to manage data access permissions precisely. RBAC systems allow you to control who has access to specific information and when, reducing the risk of unauthorized access.

Conducting regular audits and risk assessments allows you to identify weaknesses in your security systems on an ongoing basis and make necessary corrections. Companies need to be aware of data protection laws, such as the GDPR in the European Union and the CCPA in California. Compliance with these regulations not only protects your business from fines, but also builds customer trust. Regular training of employees on security threats and best practices is crucial to maintaining a high level of data protection. Implementing these steps helps you create a comprehensive cloud data security strategy that protects against a variety of threats and ensures regulatory compliance.

Hazard and risk analysis. Cloud data security for GIS is exposed to a variety of threats. The most common threats include malware attacks, which can infect GIS systems, leading to data loss or corruption. Ransomware attacks are also a significant threat, as cybercriminals can encrypt GIS data and demand a ransom to unlock it. Phishing is another method that can lead to unauthorized access to GIS data by impersonating trusted sources. Denial-of-service (DoS) attacks can disrupt the availability of GIS systems, preventing them from functioning normally. Improper cloud configurations can lead to unauthorized access to data, and insider threats such as employee actions can intentionally or accidentally compromise data (Grzegorek, 2018; Management, Support, and Quality for Business, 2024).

The risk assessment associated with individual risks includes an analysis of their potential impact on GIS systems. Malware attacks can lead to a loss of data integrity, which can result in erroneous analyses and decisions based on incorrect data. Ransomware attacks can cause you to lose access to critical GIS data, which can disrupt operations and require significant resources to recover your data. Phishing can lead to credential theft, which allows unauthorized access to GIS systems and potential data leaks. Denial-of-service attacks can disrupt the availability of GIS systems, which can have a critical impact on operations that require constant access to data. Improper configurations can lead to unauthorized access to data, which can result in data leakage or corruption. Insider threats can lead to intentional or accidental data breaches, which can have a variety of outcomes, depending on the nature of the breach (Editorial Team PortalwSieci.pl, 2024, ISO/IEC 27017:2015, 2015).

Risk assessment allows you to identify and classify threats and assess their potential impact on GIS systems, which is critical to developing effective risk management and data protection strategies.

Data protection in the cloud. Cloud data protection refers to a set of practices, technologies, and policies designed to protect data stored and processed in cloud environments from unauthorized access, loss, modification, and other threats. This includes both data at rest and data in transit.

Data encryption is an essential mechanism for protecting information. It consists in encoding data in such a way that it is unreadable to unauthorized persons. This process covers both data at rest and in transit, providing comprehensive protection against unauthorized access. Access control is a key element in protecting data from unauthorized access. It uses mechanisms such as multi-factor authentication (MFA) and identity management (IAM) that restrict access to data to authorized users only. Secure storage

and management of encryption keys is essential to maintaining data integrity and confidentiality. Effective key management includes regular key rotation and the use of advanced storage methods. Regular monitoring and auditing of access to data and activities related to data processing is crucial for detecting and preventing potential threats. Security audits allow you to identify weaknesses and implement appropriate countermeasures. Creating regular backups of data and planning recovery procedures in the event of a disaster is an indispensable part of a security strategy. This ensures the continuity of GIS operations and minimizes the risk of data loss. Applying the above practices and standards to cloud data management is critical to ensuring data security. In the context of GIS systems, appropriate security allows for effective management of geographic information, minimizing the risk of unauthorized access and data loss.

Data protection at rest involves encrypting data stored on cloud servers. This encryption ensures that data is unreadable to unauthorized people even when it's not actively being used. This is a key element to protect against unauthorized access to stored information. Data protection in transit refers to the encryption of data in transit between a user and a cloud server. This process protects the data from interception and unauthorized access during transmission. Encryption in transit is essential for ensuring the security of communications in a cloud environment. Data protection in use is about securing data processed in real time. This includes mechanisms that ensure the integrity and confidentiality of data during processing operations. This is important to protect your data from unauthorized access and manipulation during active use.

Cloud data protection provides enhanced security, protecting it from unauthorized access and security breaches. With advanced encryption and access control mechanisms, your data is better protected against potential threats. Another benefit is regulatory compliance, which means meeting legal requirements and industry standards. Protecting data in the cloud allows organizations to avoid sanctions and maintain compliance with applicable regulations, which is crucial for their legitimate functioning. Cloud data protection also ensures increased availability and reliability, which guarantees continuous access to data even in the event of a disaster. This allows organizations to operate without interruption, which is crucial for their efficiency and operational continuity. Last but not least, flexibility and scalability allow you to easily adapt your resources to changing business needs. Protecting data in the cloud allows for optimal use of resources and quick response to changing market conditions, which is crucial for dynamically growing organizations.

One of the main challenges is the complexity of management, which results from the need to manage a variety of cloud environments and tools. Organizations need to integrate and manage different platforms effectively, which can be complicated and time-consuming. Another challenge is trust in cloud providers. Organizations need to ensure that cloud providers have the right data protection measures in place to keep it secure. Choosing the right provider is crucial to maintaining a high level of data protection. Encryption key management is another essential aspect that involves secure storage and management of encryption keys. This is crucial for maintaining data integrity and confidentiality. Organizations must implement effective key management procedures to

ensure their security. The final challenge is regulatory compliance, which means meeting regulatory requirements in different jurisdictions. Organizations need to comply with different legal regulations, which can be difficult and resource-intensive. Compliance with regulations is crucial for legal functioning and avoiding sanctions.

Applying the above practices and standards to cloud data management is critical to ensuring data security. In the context of GIS systems, appropriate security allows for effective management of geographic information, minimizing the risk of unauthorized access and data loss.

The first step is to choose the right cloud provider that offers advanced data protection mechanisms. It is important that the supplier meets the highest security standards and has the appropriate certifications, which ensures confidence in their services. Another practice is to encrypt data, both at rest and in transit. Encryption ensures that data is unreadable to unauthorized persons, which protects it from interception and theft. This is a key part of protecting data in the cloud. Multi-factor authentication (MFA) is another key component that involves implementing MFA for all users who have access to data in the cloud. MFA increases security by requiring users to provide more than one means of authentication, making unauthorized access more difficult. Regular security audits are essential to maintain a high level of data protection. Conducting regular security audits and reviews allows you to identify potential threats and implement appropriate countermeasures, which minimizes the risk of breaches.

Case study. An example of the implementation of cloud data security practices and standards in GIS was a project carried out by a company (known to the authors of this study), which decided to migrate its GIS systems to the cloud. The aim of the project was to increase the availability and scalability of GIS data, while ensuring its security. As part of the implementation, ISO 27001, ISO 27017 and ISO 27018 standards were used to ensure compliance with international information security standards. Key practices included the implementation of multi-factor authentication, end-to-end encryption, and advanced monitoring and access management tools. In addition, regular security audits and training were conducted for employees to increase their awareness of data security risks and best practices.

The implementation of cloud data security practices and standards in the GIS system has brought tangible benefits to the company. Analysis of the results showed that the number of security incidents decreased significantly and GIS systems became more resilient to cyberattacks. Multi-factor authentication and end-to-end encryption effectively protected data from unauthorized access and loss of integrity. Monitoring tools enabled rapid detection and response to potential threats, which contributed to the level of data security. Regular audits and training for employees increased their awareness of the risks and improved compliance with safety procedures.

Findings from this case indicate that the application of international standards and best practices for data security in the cloud is critical to protecting GIS. Organizations should invest in advanced technologies and regular training to ensure effective data protection. Further research and development of new methods of data protection, such as

the integration of artificial intelligence and machine learning, can further enhance the security posture of GIS systems in the cloud.

Discussion

The results of the analysis confirm the effectiveness of the applied practices and standards for data security in the cloud, which is consistent with the existing literature on the topic. Studies have shown that advanced authentication and encryption mechanisms are crucial for protecting data in the cloud (Ahmadi, 2024; Sudha et al., 2022). However, the analysis also revealed some limitations of the study. First of all, the study was mainly based on data collected from incident reports, surveys and interviews, which can introduce some biases. In addition, the study did not take into account all possible threats, such as specific attacks on cloud infrastructure, suggesting the need for further research in this area (Ahmadi, 2024).

Implications for the practice include the need to continuously monitor and update security procedures to keep up with the rapidly changing threat landscape. Organizations should also invest in employee training to increase their awareness of cloud data security risks and best practices (Young, 2013). Further research should focus on the development of new technologies and methods of data protection, such as the integration of artificial intelligence and machine learning into security systems, which can significantly improve the effectiveness of GIS data protection in the cloud (Commvault).

Conclusions and recommendations

To sum up, the security of data in the cloud and GIS cloud environments are key elements of a modern IT management strategy. It requires the use of advanced technologies, procedures, and best practices to protect data and cloud resources from a variety of threats. Effective protection of cloud environments is essential to ensure the integrity, confidentiality and availability of data and business continuity.

The analysis showed that the implementation of advanced authentication mechanisms such as two-factor authentication (2FA) and end-to-end encryption significantly increases the level of GIS data protection in the cloud. Monitoring tools such as SIEM enable effective detection and response to potential threats, which helps reduce the number of security incidents.

IAM systems allow for precise management of authorizations and access to GIS data, minimizing the risk of unauthorized access. Regular backups and recovery plans ensure that your GIS continues to operate even in the event of a disaster or attack. To improve cloud data security for GIS, organizations should invest in advanced authentication and encryption technologies, implement monitoring and access management systems, regularly conduct security audits and training for employees, and back up data and develop recovery plans. Further research in the area of cloud data security for GIS should focus on the development of new technologies and methods of data protection, such as the integration of artificial intelligence and machine learning into security systems, the

analysis of specific risks to cloud infrastructure, and the study of the effectiveness of different security practices and standards in different contexts.

Compliance with international standards and regulations is crucial to ensure cloud data security for GIS, minimizing the risk of breaches and ensuring compliance with applicable regulations. Implementing cloud data security practices and standards in GIS has tangible benefits, including reducing security incidents and increasing the resilience of GIS to cyberattacks.

The results of the analysis confirm the effectiveness of the applied practices and standards for data security in the cloud, which is consistent with the existing literature on the topic. The implications for the practice include the need to constantly monitor and update safety procedures and invest in training for employees.

Further research should focus on developing new technologies and methods of data protection and analyzing the specific risks to cloud infrastructure. Compliance with international standards and regulations is crucial to ensure cloud data security for GIS, minimizing the risk of breaches and ensuring compliance with applicable regulations.

Acknowledgements

This work was financed/co-financed by Military University of Technology under research project UGB 531-000023-W500-22.

References

Ahmadi S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15, 148–167. ssrn.com, scirp.org.

Commvault. A guide to one-click cloud app recovery with Commvault Cloud Rewind. https://www.commvault.com/resources/ebook/ransomware-reversal [access: 04.02.2025].

Editorial Team PortalwSieci.pl (2024). Data Security in the Cloud – Key Aspects and Tips. PortalwSieci.pl. https://portalwsieci.pl/bezpieczenstwo-danych-w-chmurze/ [access: 06.02.2025].

Ellipsis Drive. How does GIS and cloud computing work together? https://ellipsis-drive.com/blog/how-does-gis-and-the-cloud-work-together/ [access: 14.03.2025].

GIS Cloud (2017). How Secure is to Store Data in the Cloud? GIS Cloud. https://www.giscloud.com/blog/ask-an-engineer-how-safe-is-to-store-data-in-the-cloud-and-other-safety-tips/ [access: 04.03.2025].

Grzegorek A. (2018). Bezpieczeństwo oraz aspekty prawne przetwarzania danych w chmurze obliczeniowej (*Security and legal aspects of data processing in cloud computing*). Studia Iuridica, pp. 149–163, DOI: 10.5604/01.3001.0011.7592.

ISO/IEC 27017:2015 (2015). Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/standard/43757.html [access: 06.02.2025].

Markiewicz A. (2025). Bezpieczeństwo danych w chmurze w 2025 roku. Inowroclaw.info.pl. https://inowroclaw.info.pl/artykul/bezpieczenstwo-danych-n1664486 [access: 07.03.2025].

Management, Support and Quality for Business (2024). ISO 27017: Key Principles of Cloud Security. bbquality.pl, https://www.bbquality.pl/iso-27017/ [access: 04.03.2025].

Ndamukunda J. (2024). GIS and Security. EthicalGEO. https://ethicalgeo.org/gis-and-security/ [accessed: 04.04.2025].

Orca Security (2022). 2022 Cloud Security Report. cloudsecurityalliance.org, https://orca.security/wp-content/uploads/2022/03/Orca-2022-Cloud-Security-Alert-Fatigue-Report.pdf [access: 14.03.2025].

Spatial Post (2021). The Complete Guide to GIS Cloud Computing. Spatial Post. https://www.spatialpost.com/gis-cloud-computing/ [accessed: 09.03.2025].

Sudha C.M., Murthy D.S.R. (2022). Literature Review on Security Mechanisms for Cloud Data Applications. Journal of Emerging Technologies and Innovative Research (JETIR), pp. 154–161, https://www.jetir.org/papers/JETIR2210333.pdf [access: 14.03.2025].

USC GIS Graduate Programs (2021). GIS and the Cloud: How They Work Together. gis.usc.edu, https://gis.usc.edu/blog/gis-and-the-cloud-how-they-work-together/ [access: 24.03.2025].

Young M.E. (2013). ArcGIS Cloud Security Roadmap & Best Practices for Federal Agencies. proceedings.esri.com, https://proceedings.esri.com/library/userconf/feduc13/papers/fed_47.pdf [access: 04.04.2025].