Security Analysis of Open Source GIS Server Components in Telecommunications Applications

Goran Stamenović[1][0000-0001-6241-0425], Muzafer Saračević[2][0000-0003-2577-7927], Faruk Selimović[1][0000-0002-0367-9122], Azra Ćatović[2][/]

[1] Faculty of Information Technology, Belgrade Metropolitan University, Bulevar Svetog Cara Konstantina 80-86, 18116, Niš, Serbia
goran.stamenovic@metropolitan.ac.rs
faruk.selimovic@metropolitan.ac.rs
[2] University of Novi Pazar, Dimitrija Tucovića 65, 36300 Novi Pazar, Serbia
muzafer.saracevic@uninp.edu.rs
a.catovic@uninp.edu.rs

Abstract. Telecommunications have become essential to our daily lives because ongoing technological progress has enabled innovative ways to communicate, access information and connect. The rapid advancement of telecommunications requires innovative methods for addressing challenges in network design and optimization. Geographic Information Systems (GIS) play a crucial role in telecommunication network planning and management by linking technological capabilities with their geographical contexts. Open-source geographic information systems offer organizations a budget friendly and adaptable solution to proprietary systems, fostering both innovative development and community driven software advancements. The open-source nature of GIS software creates significant security risks because it exposes critical telecommunications information to potential threats. This study examines how open-source Geographic Information Systems can improve the operational efficiency of telecommunications systems while addressing key aspects of data confidentiality and security. Within the context of telecommunication applications, this study conducts a methodical analysis of the security mechanisms present in open-source GIS server components, including GeoServer, MapGuide Open Source, Mapnik, MapServer and OpenLayers.

Keywords: Security, Geographic Information Systems (GIS), Open-source GIS software, Telecommunications

1. Introduction

Today, in our connected world, telecommunications networks are more than just convenient. They are essential for communication in cities, suburbs and rural areas. To effectively establish and improve these networks, studying the local geography is crucial. This helps in understanding where signals reach, how strong they are and what customers need. Geographic Information Systems (GIS) play a vital role in analyzing spatial factors that influence both network performance and cybersecurity. These tools help visualize and analyze geographic data, making it easier to plan and enhance networks. Geographic Information Systems are increasingly important for planning,

Research Paper
DOI: https://doi.org/10.46793/BISEC25.201S
Part of ISBN: 978-86-89755-40-4

management and service delivery in telecommunications [1]. Numerous commercial software options are available to address issues like coverage, security, and failure probability, each with its own features. While these programs are useful for telecommunications planners, the costs and time involved in customizing them can be significant disadvantages. It is also important to recognize that telecommunication systems pose notable security risks.

Various specialized software are used to determine the propagation and range of telecommunication signals. The use of this software is usually limited to a specific and well-educated group of users. The use of signal prediction techniques has resulted in substantial savings in terms of time, money, and human effort. This results in a notable increase in efficiency, fulfilling the primary goal set during the implementation of these systems. They range from less specialized to highly advanced solutions. Various commercial software options are available, such as CellOpt, SAFCO/ComOpt (automatic frequency planning), Cellular Expert/Hnit-Baltic (planning, optimization, and analysis of telecommunications networks on the ESRI ArcGIS platform), GRANET (GRAphical Radio Network Engineering Tool)/GTE Laboratories (enables planning of mobile and radio networks), Network Planner WorkPlace/Multiple Access Communications Ltd (high-resolution planning of mobile and wireless networks in urban areas), PathPro/MLJ Software (designing wireless telephone networks), Quotient/Quotient Communications (designing, implementation and optimization of telecommunication networks). The main limitations of these professional tools are their high costs and the lengthy implementation times required for potential changes or modifications to system features tailored to user needs.

Open-source software is significantly cheaper than commercial software for the same features and functions [2]. Furthermore, flexible and adaptable, open-source systems are capable of being more responsive to specific needs. The source code can be analyzed, modified and new modules can be added. This paper's objective is to look into the possibilities of implementing open-source Geographic Information Systems for operational efficiency in telecommunications, as well as addressing important issues of data confidentiality and security. Open-source Geographic Information System is an alternative to commercial software, especially when it comes to price. Users can move into a system that is responsive in terms of flexibility and support from the community. Several open-source GIS systems are perhaps more common and renowned globally pertaining to discoveries made in telecommunications for spatial data analysis. Some of these include GRASS GIS, gvSIG, Quantum GIS and JUMP/OpenJUMP. As with any valuable tool, security concerns must be addressed to maintain the confidentiality and integrity of sensitive data and sensitive geographic information can be intercepted and accessed without encryption.

The telecommunications industry faces a significant risk of being targeted by malicious actors due to the sensitivity of its data, such as user geolocation, network infrastructure, and service usage. Violations of data integrity and confidentiality are always harmful, and the negative impacts of such breaches can include reputational damage, financial loss, and unauthorized privacy invasion. This research will develop a proactive security

module for an open-source geographic information system server component in telecommunications. The aim is to create a security framework that is robust enough to resist breaches and adaptable enough to grow with the open-source movement.

The adoption of open-source GIS provides cost savings and flexibility but also introduces significant security challenges. Open-source GIS solutions offer an affordable and adaptable alternative to proprietary systems, fostering innovation and community-driven development [3]. This study conducts a systematic analysis of security measures used in popular open-source GIS server technologies (GeoServer, MapGuide Open Source, Mapnik, MapServer and OpenLayers) within the context of telecommunication applications. While utilizing open-source GIS server components can save costs and enhance flexibility, there are serious security risks involved. We evaluate authentication, authorization, data security, network hardening, and vulnerability management capabilities against telecom-specific threats (e.g., infrastructure sabotage, subscriber data leakage, and service disruption) [4].

Open-source GIS software used in telecommunications implements server components for spatial data processing:
- GeoServer: manages cell-tower locations via WMS/WFS services
- MapGuide: visualizes fiber-optic networks
- Mapnik/MapServer: renders real-time network coverage maps
- OpenLayers: web client for field technician portals

2. GeoServer - Open-Source Geospatial Web Server

GeoServer is an open-source web server developed in Java that enables users to share, process, and edit geospatial data. It is a comprehensive implementation of several open standards, most notably the Web Feature Service (WFS), Web Map Service (WMS) and Web Coverage Service (WCS). Owing to its high level of interoperability, GeoServer can distribute data from widely used spatial data sources that adhere to open standards. It also allows integration with virtual globes, such as Google Earth and NASA World Wind, as well as with popular web-based mapping frameworks, such as OpenLayers, Google Maps, and Bing Maps [5]. Using standard protocols, GeoServer enables the download and dissemination of data in multiple formats, including KML, GML, Shapefile, PDF, GeoJSON, JPEG, GIF and PNG [5]. Its security mechanisms include authentication (supporting LDAP, OAuth 2.0 and database-based systems), data protection (via SSL/TLS encryption for WMS/WFS services and AES-256 encryption for credential storage) and regular security updates [6].

Nevertheless, GeoServer is subject to certain vulnerabilities, including unauthenticated XML External Entity (XXE) attacks through WFS requests, weak password hashing mechanisms, and potential exploits through administrative interfaces [7]. Security can be enhanced by enabling Role-Based Access Control (RBAC), deploying a reverse

proxy (e.g., NGINX) to filter malicious OWG requests and maintaining frequent updates to the latest stable version [5].

The latest stable version of GeoServer is version 2.27.1 (May 2025)

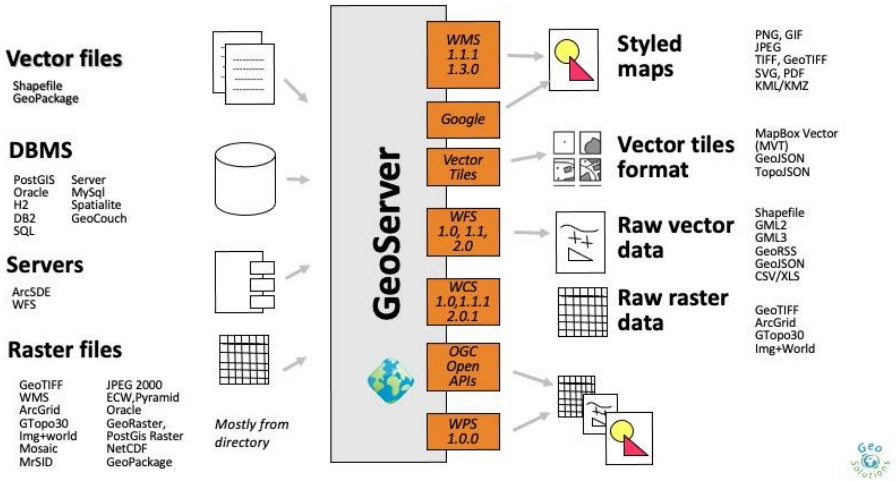

Fig.1. GeoServer interface (source: https://www.geosolutionsgroup.com/technologies/geoserver)

3. MapGuide Open Source - Web-Based Geospatial Platform

MapGuide Open Source is a web-based platform that enables users to develop and deploy web mapping applications while utilizing geospatial services. Although it shares a name with Autodesk's commercial MapGuide product, MapGuide Open Source (MapGuide OS) is a completely new project that features a unique codebase and an open-source licensing model. Autodesk sold its commercial version of MapGuide, offering additional features such as support for more formats, official product support, and improved compatibility with legacy systems, until early 2018. Since then, MapGuide's development has continued under the open-source model [8]. MapGuide OS offers an interactive viewer that supports feature selection, map interaction, and spatial operations such as buffering, querying, and measuring. The platform uses an XML-based content repository and supports a wide variety of geospatial file formats, databases and standards. It can run on both Linux and Windows operating systems, supports Apache and IIS web servers, and includes APIs in PHP, .NET, Java, and JavaScript for application development [8]. As a newer product, MapGuide features a more modern architecture than its predecessor, MapServer, and incorporates standardized web interface components that enhance user-friendliness [8].

However, potential security vulnerabilities include susceptibility to SQL/XML injection, weak password configuration, inadequate session management, lack of HTTPS encryption, and improper configuration of OGC standards (WMS, WFS), which can result in denial-of-service (DoS) attacks [9]. Security enhancements for MapGuide OS should include the enforcement of HTTPS/TLS, integration with OAuth 2.0 or SAML for centralized access control, implementation of Attribute-Based Access Control, restriction of access to WMS/WFS services, and mitigation of DoS attacks through tools such as ModSecurity [10].

The latest stable release of MapGuide Open Source is version 3.1.2, released in March 2019.

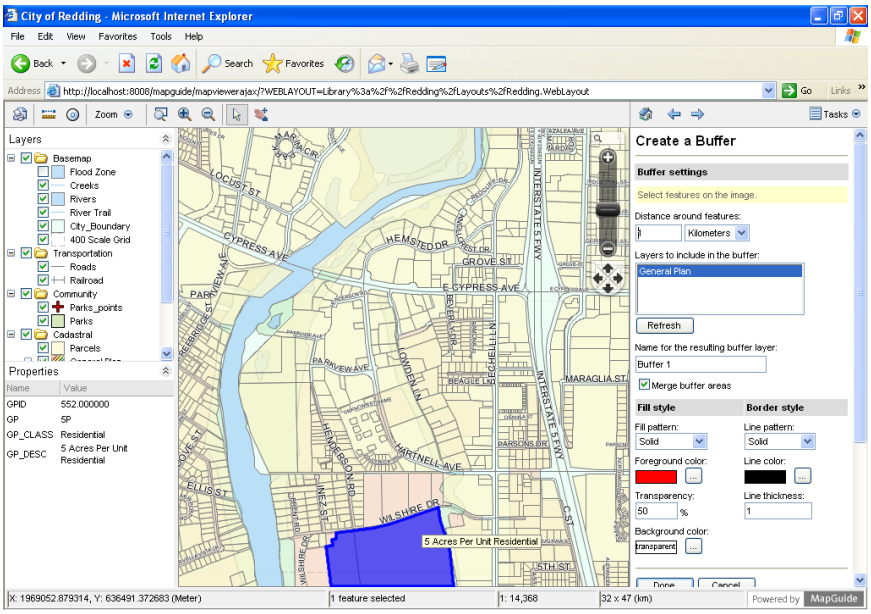

Fig.2. MapGuide Open Source (source: https://www.osgeo.org/projects/mapguide-open-source/)

4. MapNik - Open-Source Map Rendering Software

Mapnik is an open-source software library designed for high-quality map rendering. Developed primarily in C++, it supports scripting in several programming languages, including JavaScript (Node.js), Python, Ruby, and Java. It leverages the Anti-Grain Geometry rendering engine and supports a wide array of geospatial data formats, including ESRI Shapefiles, PostGIS, and TIFF. osm files, GDAL/OGR datasets and CSV files. Mapnik is used to render the default layer on the OpenStreetMap website.

This involves processing raw OpenStreetMap data and applying a stylesheet to generate the visual representation of the map. The library supports multiple output formats, including PNG, JPEG, SVG, and PDF, and enables the flexible styling and design of various map types. On the OpenStreetMap platform, Mapnik generates thousands of 256×256 pixel raster tiles, which are displayed through a JavaScript-based Slippy Map interface [11].

From a cybersecurity perspective, Mapnik presents certain vulnerabilities. These include vector graphics injection attacks via SVG symbols and denial-of-service attacks triggered by infinite loops embedded in malicious GeoJSON files. Several mitigation strategies are recommended to enhance the security posture of Mapnik-based applications. These include the deployment of Web Application Firewalls (WAFs) to filter and block malicious Open Geospatial Consortium (OGC) requests, such as WMS and WFS, as well as the implementation of file system restrictions by setting files to read-only mode within Docker containers.

The latest stable release of MapNik is version 4.1.0. (Jun 2025).

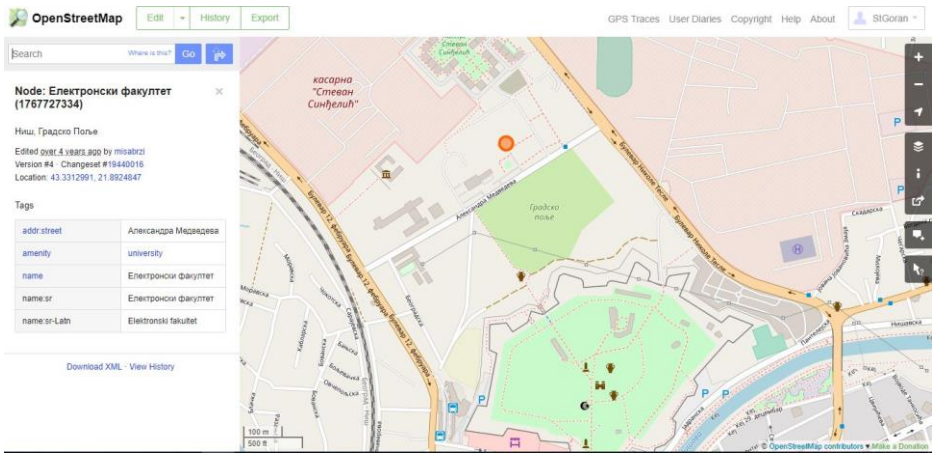

Fig.3. OpenStreetMap using Mapnik engine (source: https://www.openstreetmap.org/)

5. MapServer - Open-Source Framework for Web-Based Geospatial Applications

MapServer, originally developed at the University of Minnesota, is an open-source platform designed for building web-based geospatial applications. It runs on multiple operating systems, including Linux, Windows, and macOS. Often regarded as one of the most successful open-source GIS projects, MapServer was initially created with support from NASA, which aimed to make satellite imagery accessible to the public.

Written in C, MapServer enables the creation of geographic maps that can direct users to targeted content. It has a multidisciplinary and active developer community, with some core contributors working full-time to maintain and enhance the platform. The project is well documented, continuously updated and increasingly modular with each release. MapServer supports a wider range of input data formats than many competitors and offers strong performance with easy installation and configuration. Its key features include robust support for raster and vector data via GDAL/OGR, compatibility with various Open Geospatial Consortium standards and extensibility through multiple scripting languages such as PHP, Python.NET and Perl. It supports advanced rendering engines like AGG and Cairo and integrates numerous OGC and web mapping standards, including Filter Encoding, GeoJSON, GeoTIFF, Geography Markup Language (GML), Keyhole Markup Language (KML), OpenStreetMap (OSM), Styled Layer Descriptor (SLD), Sensor Observation Service (SOS), Web Coverage Service (WCS), Web Feature Service (WFS), Web Map Context (WMC) and Web Map Service (WMS).

MapServer provides security features, such as support for HTTP Basic/Digest authentication, OAuth 2.0, and LDAP integration via .map files. It also includes built-in protections against buffer overflow vulnerabilities and automatic sanitization of HTML and SVG to prevent cross-site scripting (XSS) attacks. Despite its robust capabilities, there are several security risks. These include unauthorized filter injection in WMS/WFS requests, XML-based attacks via SLD files, and misconfigured proxy parameters that may allow internal network scanning. To mitigate these threats, security best practices for MapServer include Enabling Content Security Policy to block script execution in map files, Deploying MapServer through mod security or within Docker containers, and rejecting requests that involve highly complex polygon geometries (e.g., polygons with over 10,000 nodes) to prevent denial-of-service attacks.

The latest stable version of MapServer is version 8.4.0. (Jan, 2025).

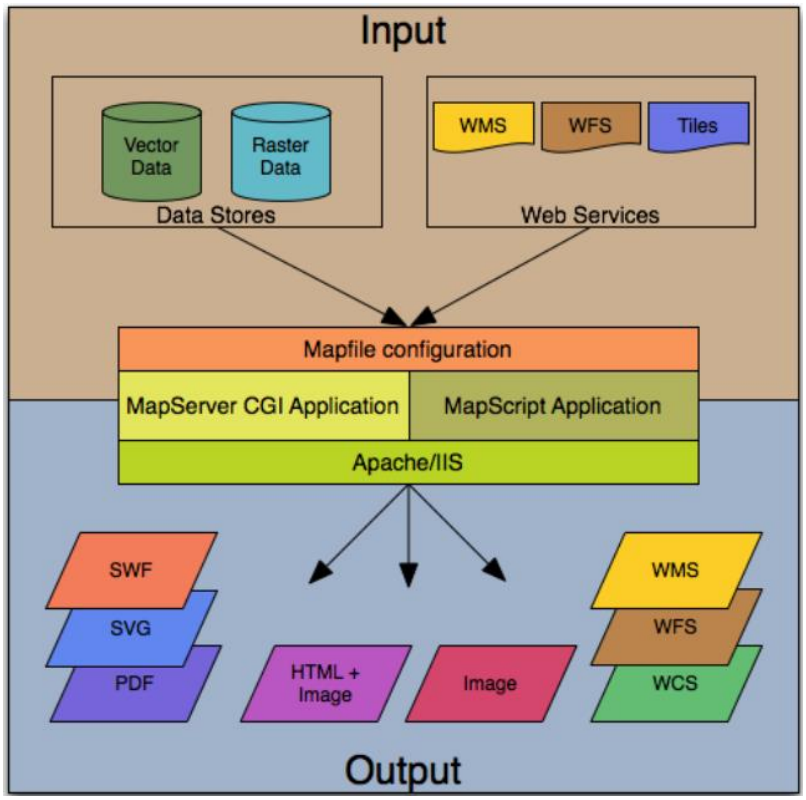

Fig.4. MapServer architecture (source: https://download.osgeo.org/mapserver/docs/MapServer.pdf)

6. OpenLayers - Web-Based JavaScript Library for Geospatial Visualization and Secure Application Design

OpenLayers is an open-source JavaScript library designed to render spatial data in web browsers. It provides a robust application programming interface for developing feature-rich, interactive geographic web applications, similar in functionality to platforms such as Google Maps and Bing Maps. Within the GeoServer, OpenLayers serves as an integrated client for visualizing the geospatial data layers. In the context of the software module under development, suitable Web Map Service (WMS) endpoints were employed to render the digital elevation model of the terrain relevant to radio signal propagation. Web Feature Service (WFS) endpoints were used to retrieve and display vector data in the appropriate formats. By combining the elevation data retrieved from these services with relevant mathematical models for radio signal propagation, the resulting visualization accurately delineates the area covered by the wireless telecommunications transmitter. Examples of the applied WFS services

include a service that returns rasterized data in the form of point collections and a service that is responsible for map area clipping to delineate the signal coverage zone. Regarding visualization strategies, the research explores both 2D and 3D rendering capabilities, as well as the integration of a temporal dimension through animation techniques to support the spatiotemporal data representation [12].

The security architecture is fully web-based with no direct access to the server infrastructure. This includes the strict enforcement of Content Security Policies and the mandatory use of HTTPS protocols for all data transmissions. Despite these safeguards, OpenLayers based applications may face security risks, such as poor proxy configuration, which could allow unauthorized request redirection and unprotected write operations during geodata modification, potentially leading to data integrity issues. As a client-side library, OpenLayers cannot directly manage server-side data security; however, it plays a critical role in securing client-server communication and protecting client-side data integrity. Best practices for enhancing OpenLayers security include the mandatory use of HTTPS for all WMS/WFS requests, implementation of subresource integrity for all external scripts, integration with OAuth 2.0 for access control, and immediate memory clearance following the handling of security-sensitive information. These measures establish OpenLayers as a reliable platform for high-security web mapping applications, including those used in the defense, healthcare, and financial sectors.

The latest official release of OpenLayers is version 10.5.0, published in January 2025 [12].

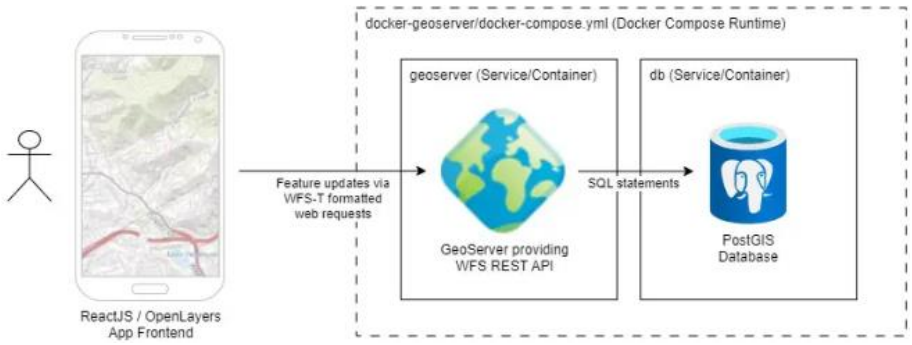

Fig.5. OpenLayers (source: https://taylor.callsen.me/save-openlayers-feature-data-to-postgis-using-wfs-transactions/)

7. Discussion

Geographic Information Systems are used to solve many problems in the telecommunications industry; however, the high cost of commercial GIS software often limits access for many users. Open-source GIS provides a more affordable and practical

option, enabling a wider range of people to use advanced tools. A major advantage of open-source GIS is its ability to be customized. The open architecture allows users to modify the software to meet their specific needs, making the tools better suited to different types of projects. This is especially important because telecom projects can vary greatly in their goals and scope. Open-source communities collaborate, fostering new ideas and enhancements in GIS applications for telecommunications. Open-source GIS is more flexible, as users can analyze, change, or add new features to the code as needed. This supports better customization and continuous upgrades. Components like GeoServer, MapGuide OS, Mapnik, and MapServer, along with client libraries such as OpenLayers, are scalable options compared to proprietary solutions. However, integrating these into telecom systems that handle sensitive data, such as infrastructure details and user locations, requires strict security measures. Recent events, such as those reported by Hernández et al. in [13], have underscored the risks associated with geospatial data exposure.

Table 1. Overview of Security Mechanisms in Open-Source GIS Server Components (Source: Author)

Component	Authentication & Authorization	Encryption (TLS/SSL)	Audit Logging	Vulnerability Management	Notes
GeoServer	LDAP, JDBC, RBAC *	Supported (via config)	Supported (plugin)	Active community, regular updates	Most complete built-in security
MapGuide Open Source	HTTP Authentication, RBAC	External web server	Limited native, external needed	Active community, slower release cycle	Depends on an external web server for encryption
Mapnik	None (external)	External web server	None (external)	Active project	Lightweight, security depends on integration
MapServer	Config-based	External web server	Limited native, external needed	Moderate update frequency	Needs careful configuration to avoid leaks
OpenLayers	N/A (client-side)	N/A (depends on API server)	N/A	Frequent updates	Security is enforced entirely on server and API endpoints

** LDAP – Lightweight Directory Access Protocol, JDBC – Java Database Connectivity, RBAC – Role-Based Access Control*

Looking at GeoServer, MapGuide, Mapnik, MapServer and OpenLayers, there are both similarities and differences in how they are structured, which affects where they might be more or less secure. GeoServer stands out as a better option for users who need

strong security settings. The other tools often need more complex setup with external systems like NGINX, Apache, or IAM solutions that are more common in larger businesses. For telecom companies, using GeoServer with LDAP and Role-Based Access Control along with MapGuide Open Source, Mapnik or MapServer as the rendering tools, and secure middleware as the front end, would be the most suitable choice. Other recommendations include the enforcement of HTTPS/TLS for all services, regular security audits, penetration tests, and centralized logging with the use of Security Information and Event Management (SIEM) systems. SIEM systems support the combination with other systems and security tools enabling the automation of reactive measures on some actions like the detection of malicious traffic or compromised systems [14]. A compromised GIS server component can initiate cascading failures in critical telecommunication services. For instance, if the GIS system is responsible for real-time network monitoring and fault detecting, its failure can cause significantly erroneous operational data, wrong maintenance actions, or erroneous system shutdowns based on incorrect information. For example, an attacker exploiting a vulnerability in GeoServer can inject false network topology data, causing routing errors or service outages. Furthermore, if GIS is integrated with service provisioning systems, a breach could enable unauthorized service activation or deactivation, directly impacting subscribers. The accuracy of geospatial data is crucial during network planning and engineering. Incorrect data can cause slow network growth or the wrong use of resources, which ultimately leads to inefficiency and increased expenses over time. GIS components can also be targets of denial-of-service attacks, making mapping and management tools unavailable and disrupting network incident response or daily operations [4]. The attack surface is significantly widened by the architectural features of open-source GIS servers. Rather than being monolithic, these systems consist of several modules which interact with each other such as; web and application servers, geospatial data store, and a myriad of other libraries [15]. The open-source nature of the GIS bestows the flexibility to tailor the software to the different problems posed by the analysis of the spatial data.

The architecture of open-source GIS server components directly influences their vulnerability to potential attacks. These systems are not single, unified programs but are made up of multiple modules like web servers, application servers, geospatial databases and various libraries [15]. This modular design gives them flexibility, allowing users to tailor the software to specific needs in spatial data analysis. The structure of these open-source GIS servers directly affects their vulnerability to attacks. Unlike monolithic systems, these systems are built from multiple components, each of which could be a potential entry point for attacks. By inviting contributions from a broad community of developers and researchers, these projects remain at the forefront of technological advancements, consistently delivering updated features and methodologies. Nevertheless, the very openness that drives progress can also expand the system's attack surface, making the integration of comprehensive security mechanisms not just beneficial, but essential for ensuring the reliability and integrity of future telecommunications infrastructure.

8. Conclusion

The telecommunications industry's increasing reliance on geospatial technologies has undeniably enhanced efficiency in areas such as network planning, disaster management and service delivery. Nonetheless, open-source GIS server components present distinct security concerns, particularly because their architecture typically incorporates web servers, application servers, and spatial databases, each of which may serve as a potential attack vector. Common vulnerabilities, including misconfigured systems, default login credentials and outdated software, are well-documented risks [16]. Furthermore, the integration of multiple open-source components can inadvertently introduce additional security gaps.

The diverse landscape of open-source GIS implementations in telecommunications creates significant challenges in establishing unified security measures. Operators often use a mix of proprietary and open-source software, along with different operating systems and a variety of network setups. The lack of standardization makes it difficult to create a consistent security baseline for open-source GIS systems. Consequently, organizations must develop custom security solutions, which are both time-consuming and prone to inconsistencies. Addressing these issues requires a comprehensive framework to evaluate risks and apply controls across various technologies, using universal security principles and flexible automated tools [17, 18].

This study evaluates vulnerabilities in widely used open-source GIS environments, including unencrypted data, weak access controls and outdated authentication. It identifies these security issues and provides practical solutions. These problems pose real risks in modern telecom settings. To address these challenges, we implemented targeted solutions such as role-based geospatial encryption, zero-trust frameworks for data sharing, and blockchain-based metadata verification. As 5G and 6G deployments accelerate globally, the integration of robust, community-supported security measures within open-source GIS systems becomes increasingly vital for ensuring broad and equitable network access. Looking forward, continued advances in artificial intelligence and cloud technologies are poised to further transform network planning, reinforcing the central role of open-source GIS in driving innovation across the telecommunications landscape.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Goodchild, M. F., Citizens as sensors: The world of volunteered geography, GeoJournal, 69 (4), 211–221. https://doi.org/10.1007/s10708-007-9111-y, (2007).
2. Spinellis, D., & Giannikas, V., Organizational adoption of open source software. Journal of Systems and Software, 85(3), 666–682. https://doi.org/10.1016/j.jss.2011.09.037, (2012).
3. Sandhya, M. C, Exploring Opportunities with Open Source GIS, International Journal of Engineering Research and, vol. V9, no. 05. ESRSA Publications Pvt. Ltd., doi: 10.17577/ijertv9is050545, (2020).
4. Buczak, A. L., & Guven, E., 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, (2016).
5. GeoServer. GeoServer 2.27.1 release notes. https://geoserver.org/release/2.27.1, (2025).
6. Turton, I., Security in GeoServer: An overview. GeoServer Blog. https://geoserver.org/blog/security-overview/, (2023).
7. National Institute of Standards and Technology (NIST), CVE-2023-XXXXX: GeoServer XXE vulnerability. National Vulnerability Database. https://nvd.nist.gov/, (2024).
8. MapServer, MapServer 8.4.0 documentation. https://mapserver.org/, (2025).
9. SecuriTeam, MapGuide OS vulnerability assessment report. https://www.securiteam.com/, (2021).
10. OWASP, Web application security risks and countermeasures. Open Web Application Security Project. https://owasp.org/, (2022).
11. Mapnik, Mapnik 4.1.0 documentation. https://mapnik.org/2025).
12. OpenLayers., OpenLayers 10.5.0 documentation. https://openlayers.org/, (2025).
13. Hernández, F. et al., Geodata Breaches in Critical Infrastructure: Analysis of 2018–2020 Incidents. IEEE Transactions on Geoscience and Remote Sensing, 59(5), 4120–4131, (2021).
14. Montesino, R., Fenz, S., & Baluja García, W., SIEM-based framework for security controls automation. Information & Computer Security, 28(3), 320–341. doi 10.1108/IMCS-08-2020-0087, (2020).
15. Steiniger, S., & Bocher, E., An overview on current free and open source desktop GIS developments. International Journal of Geographical Information Science, 23(10), 1345–1370. https://doi.org/10.1080/13658810802634956, (2009).
16. Gustavsson, T., Managing the Open Source Dependency, Computer, vol. 53, no. 2. Institute of Electrical and Electronics Engineers (IEEE), pp. 83–87, doi: 10.1109/mc.2019.2955869, (2020).
17. Tankard, C., Advanced persistent threats and how to monitor and deter them. Network Security, 2011(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1, (2011).
18. Stamenović, G., Saračević, M., Jukić, S., Kamberović, H., Implementation of Security Mechanisms in Open Source GIS Software in Telecommunications, The paper has been accepted for publication in Computer Science journal: http://journals.agh.edu.pl/csci, ISSN: 1508-2806; e-ISSN: 2300-7036, (2025).