Investigating the Role of Post-Quantum Cryptography in Enhancing Blockchain-Based Geospatial Data Exchange

Darshana Rawal[1], Jan Seedorf [1] ,Atharva Chaudhari[1] , Matthias Hamann[1]
1 - Hochschule für Technik Stuttgart, Schellingstr 24,70174 Stuttgart
rawalnet@yahoo.com, jan.seedorf@hft-stuttgart.de, atharvachaudhari7@gmail.com, matthias.hamann@hft-stuttgart.de

Keywords: Post-Quantum Cryptography, Geospatial Data, Blockchain, Interplanetary File System, Encryption, Decryption

Abstract
The rapid expansion of geospatial data from satellite images, IoT sensors, and location services has created significant opportunities for applications such as urban planning, environmental monitoring, and defence intelligence. However, the sensitive nature of geospatial data sets poses serious security challenges, including unauthorised access, data manipulation and the emerging threats of quantum computing. Traditional cryptographic systems such as RSA and Elliptical Curve Cryptography may be vulnerable to quantum attacks, which highlights the need for quantum-resistant security mechanisms. This paper proposes a hybrid architecture that integrates post-quantum cryptography, blockchains, and decentralised storage to ensure a secure and scalable exchange of geo-spatial data. The proposed system combines AES-GCM for high-performance symmetric encryption with Kyber-based key encapsulation on a lattice basis to provide quantum-proof key protection. Encrypted geo-spatial data is stored off-chain using the IPFS (Interplanetary File System), while metadata and access control policies are managed by smart contracts on private Ethereum blocks. The architecture is implemented with FastAPI back-end services, cryptographic microservices, and a web interface to interact with the user. Experimental evaluation shows a stable performance across different geospatial file sizes, with low standard deviations indicating a consistent required computing power. The results highlight the feasibility of integrating post-quantum cryptography with decentralised technologies to enable the sharing of geospatial data in a secure, scalable and resilient way in the future.

1. Introduction

Geospatial data is a complex collection of information linked to specific locations on the Earth's surface. It consists of spatial data—such as geographic coordinates—and attribute data that describe the characteristics of those features. For example, a dataset might detail the location of a lake, its depth, and the surrounding vegetation. There are two main forms of geospatial data: vector data, which includes discrete features such as points, lines, and polygons, and raster data, which represent continuous surfaces, such as satellite imagery and elevation models. Today, geospatial data is vital for various fields. Urban planners and civil engineers use it to design smart cities and optimize transportation, while environmental scientists monitor climate change and assess land use. In agriculture, it helps with crop health and soil analysis. The defence sector relies on it for mission planning and reconnaissance. As technology advances, the risk of cyber threats to sensitive geospatial data increases, making its protection a top priority. Its strategic significance has led to the exploration of distributed ledger technologies as a secure means of safeguarding it.

1.1 Blockchain: Structure, Principles, and Security

Blockchain is a distributed ledger technology (DLT) that records, stores, and shares data in a decentralized, tamper-resistant manner across a network of nodes. Initially developed for Bitcoin in 2008, it has expanded into applications across finance, healthcare, and supply chains. Each block contains transactions, a timestamp, a cryptographic hash of the previous block, and a nonce, making the data immutable once added to the chain. This structure ensures that altering one block would require changing all subsequent blocks, a task that requires consensus from the network. There are different types of blockchains: Public Blockchains (e.g., Bitcoin, Ethereum) are open to anyone; Private Blockchains (e.g., Hyperledger) are controlled by a single organization; and Consortium Blockchains (e.g., R3 Corda) involve multiple institutions for collaborative governance. Understanding these distinctions is essential for effectively leveraging blockchain technology (Antonopoulos, 2017).

1.2 Overview of Cryptography

Cryptography is a basic discipline of information and communication security. It includes a set of techniques to ensure confidentiality, integrity, authenticity, and non-repudiation of data. While encryption protects information from unauthorised access by rendering it illegible, other cryptographic mechanisms, such as digital signatures, hash functions, and Message Authentication Codes (MAC), provide authenticity and integrity validation of the data being transmitted. As digital communications and data exchange continue to grow, cryptography remains essential to establish trust and security in modern systems.

The key benefits of cryptography include: a) ***Confidentiality:*** It keeps private information, such as financial records and personal communications, secure from unauthorized access, allowing only authorized individuals to read it; b) ***Authentication:*** This verifies users' identities and the authenticity of their messages using methods such as digital certificates, fostering trust and preventing impersonation; c) ***Integrity:*** Cryptography safeguards data against alteration by using hash functions and digital signatures to detect unauthorized changes, ensuring the data remains genuine; d) ***Non-repudiation:*** It ensures that individuals cannot deny their involvement in transactions or communications, providing accountability essential in legal and financial matters.

1.3 Pre-Quantum Cryptography

The earliest methods for securing communications were mainly aimed at hiding information through various substitution and implementation techniques, often using shared secret keys, to ensure that only authorised parties could interpret messages. Although they were primarily concerned with confidentiality, these methods laid the foundations for classic cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) which also provide for the authentication, integrity and

This contribution has been peer-reviewed. The double-blind peer-review was conducted on the basis of the full paper.
https://doi.org/10.5194/isprs-annals-XI-4-2026-443-2026

non-counterfeiting of digital communications. These algorithms were designed to be secure against classical computing attacks but may be vulnerable to quantum computing threats.

1.4 Post-Quantum Cryptography Overview

Post-Quantum Cryptography (PQC) involves a new generation of algorithms designed to protect digital information from threats posed by quantum computers. Traditional systems like RSA and ECC rely on problems that are hard for classical computers but can be solved efficiently by quantum algorithms such as Shor’s algorithm (Shor, 1994). PQC seeks to create quantum-resistant algorithms that can be utilized with current digital infrastructure, ensuring data security in a future dominated by quantum technology. This paper explores the post-quantum cryptographic framework, with a particular focus on Kyber as a key encapsulation mechanism based on lattice cryptography. The study explores the use of the Kyber algorithm to securely encrypt AES symmetric keys, creating a two-layer security model that integrates quantum-proof key exchange with high-performance symmetric encryption (AES itself is considered quantum-proof if keys are of length 256 bits). The goal of this approach is to increase the resilience of cryptographic systems against potential quantum and classical attacks, while addressing the growing vulnerability of traditional cryptographic systems in today's evolving digital environment.

2. Related Literature

This literature review explores three key research areas: geo-spatial data protection, the use of blockchains to ensure data integrity and control access, and the development of quantum cryptography as a means of enhancing the security of future cryptography. The review concludes with a synthesis of the current findings and identified research gaps in these areas, which formed the basis of this study.

2.1 Existing Methods of Geospatial Data Protection

Existing geospatial data protection techniques rely mainly on encryption, such as the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA), to ensure confidentiality during the storage and transmission of geospatial data. Spatial camouflage, k-anonymity, and differential privacy are employed in location-based services to prevent re-identification. Access control models such as RBAC and digital watermarks (Sandhu et al., 1996) further promote controlled sharing and protection of data ownership. Recently blockchain systems, such as Ethereum, have been explored to improve data integrity and traceability; however, most current approaches remain centralized and lack integrated, privacy-preserving, decentralised authentication mechanisms.

2.2 Geospatial Data: Characteristics and Security Concerns

Geospatial data includes information about specific locations on the Earth's surface and is used in many fields, including urban planning, navigation, disaster response, climate analysis, defence, and precision agriculture. These data, which may include satellite images, GPS records, vector maps, and sensor data, are often large in scale and sensitive and are therefore subject to current privacy and data protection legislation (Goodchild, 1992; Elwood & Leszczynski, 2018). Given its strategic importance, geospatial data is confronted with several security challenges:

Tampering and Data Corruption: Unauthorized changes to geospatial datasets can result in incorrect interpretations, navigational errors, and misguided policy decisions. For instance, if land-use or zoning data were maliciously altered, city planners might approve construction in environmentally restricted or flood-prone zones, leading to serious legal and safety consequences.

Unauthorized Access and Espionage: Unprotected spatial data can expose sensitive information about military areas, infrastructure designs, and critical resources, thereby posing a threat to national security.

Privacy Violations: The tracking of individual movements via location-based services, when conducted without adequate anonymization, can violate data protection regulations such as the General Data Protection Regulation (GDPR), a European Union law governing personal data privacy.

As noted by Goodchild (Goodchild, 1992), although the geospatial domain has made significant progress in terms of analytical and visualization capabilities, security aspects - in particular confidentiality and fine-grained access controls - still require considerable development.

2.3 Blockchain for Geospatial Data Integrity and Access Control

Blockchain technology is a decentralized, append-only ledger that facilitates the secure, transparent, and tamper-proof recording of transactions without centralized authorities. This unique capability makes blockchain highly valuable for ensuring data integrity, conducting audits, and managing access control in systems that handle sensitive information. Several research initiatives have identified potential use cases for blockchain within geospatial data systems, including:

Land Administration Systems: By recording land ownership, transfers, and resolutions of disputes on an immutable blockchain, governments can combat corruption and enhance transparency (Paavo et al., 2025).

Environmental Monitoring: Data from distributed IoT devices—such as those used to monitor water quality or air pollution—can be securely logged on the blockchain, ensuring accountability and reliability (Udodiri et al., 2025).

Crowdsourced Mapping: Platforms like OpenStreetMap can utilize blockchain to validate and track user contributions effectively, thereby preserving a comprehensive history of edits and building trust in volunteered geographic information.

Despite its advantages, blockchain faces significant limitations when handling large or private datasets:

- On-chain data is inherently public and immutable, making it unsuitable for storing sensitive files unless they are encrypted.
- The costs associated with on-chain storage can be prohibitive, particularly for large files such as satellite imagery or topographic maps. For instance, storing even a single gigabyte of data directly on the Ethereum blockchain could cost thousands of dollars in gas fees, making it economically unfeasible for high-volume geospatial datasets.
- The use of encryption on-chain restricts the functionality of smart contracts, as these contracts cannot access encrypted data.

To mitigate these limitations, researchers are exploring solutions that involve off-chain storage in conjunction with on-chain metadata references. For example, data can be stored in systems like IPFS (InterPlanetary File System), with only the content hash or identifier recorded on the blockchain. This approach offers a way to balance integrity and confidentiality while leveraging the strengths of blockchain technology.

This contribution has been peer-reviewed. The double-blind peer-review was conducted on the basis of the full paper.
https://doi.org/10.5194/isprs-annals-XI-4-2026-443-2026 | © Author(s) 2026. CC BY 4.0 License.

2.4 Post-Quantum Cryptography (PQC)

Advances in quantum computing pose significant risks to traditional cryptographic systems. Shor's algorithm can efficiently factor large numbers and compute discrete logarithms, which directly threatens public-key cryptography such as RSA and elliptic-curve cryptography (ECC). By contrast, the generic impact of Grover’s algorithm on symmetric cryptographic schemes is a quadratic speedup for exhaustive key search, so that a k-bit key offers about k/2 bits of security against such attacks. In our setting, this can be mitigated straightforwardly by using AES-256 rather than AES-128. In response to these emerging threats, the Post Quantum Cryptography (PQC) project was created to develop cryptographic algorithms that are both resistant to classical and quantum attacks. The PQC algorithms are based on mathematical problems that are believed to be impervious to quantum computing, such as lattice schemes, hash schemes, code schemes, and multivariate polynomial schemes (NIST, 2025).

Lattice-based problems: These are considered one of the most promising avenues for post-quantum security. Noteworthy examples include:

- ***Kyber:*** A key encapsulation mechanism (KEM) that leverages the hardness of lattice problems to provide secure key exchange.
- ***Dilithium:*** A digital signature scheme that also relies on lattice structures to ensure message integrity and authenticity.

Code-based cryptography: This approach uses error-correcting codes to provide security. A prominent example is:

- ***Classic McEliece:*** A public-key encryption system that has withstood scrutiny over decades and is believed to be resistant to quantum attacks due to its reliance on the difficulty of decoding random linear codes.

Hash-based cryptography: Utilizing the properties of cryptographic hash functions, this method offers security through:

- ***SPHINCS+:*** A stateless hash-based signature scheme that provides strong security guarantees based on the robustness of hash functions.

In particular, all of these PQC algorithms do not rely on mathematical problems such as integer factorization or discrete logarithm, both of which can be solved efficiently by Shor's algorithm (Shor, 1994) using quantum computing.

In 2024, the National Institute of Standards and Technology (NIST) finalized the standardization process for post-quantum cryptographic algorithms, thereby establishing a solid foundation for secure communications and data protection in a future increasingly characterized by quantum computing (NIST, 2025).

3. Research Objectives

Geospatial data has emerged as a vital asset in modern decision-making, serving as the foundation for insights and strategies across various fields. However, as the volume of this data expands and its sensitivity intensifies, there is an urgent need for stronger protective measures. This section outlines the key challenges motivating this research and defines the objectives for developing a secure, quantum-resilient, and scalable architecture for managing geospatial data.

3.1 Problem Statement

In recent years, the generation and use of geospatial data have grown significantly due to the widespread availability of satellite imagery, drone surveillance, sensor networks, and mobile location services. This data is critical for various applications, including urban infrastructure, climate monitoring, transportation, agriculture, and military operations. However, the sensitive nature of geospatial data makes it a prime target for cyberattacks, unauthorized access, and data tampering—as demonstrated by incidents such as the well-known 2023 breach of U.S. government geospatial systems, which exposed critical mapping and infrastructure data.

Traditionally, many digital systems have been secured by RSA and ECC, but with advances in quantum computing, these may not be secure in the future. Shor's algorithm (Shor, 1994) shows that such quantum computers can effectively break the public key encryption algorithms that protect many geospatial systems.

Moreover, while blockchain provides a tamper-proof ledger technology suitable for recording and controlling access, it does not provide a natural guarantee of confidentiality. Most blockchains are transparent by design, which means that all data on the chain is accessible to the public. Therefore, storing raw, unencrypted geospatial data on the chain can violate privacy rules and risk unintentionally exposing sensitive information At the same time, encrypting and storing data directly on a blockchain introduces challenges such as high storage costs, limited privacy controls, and rigid key management..

The existence of this situation highlights a significant research gap: what is the best way to create a scalable, future-proof architecture for secure access, sharing, and control of geospatial data, while protecting against quantum threats and ensuring data integrity? Existing approaches often lack performance, privacy, or postquantum resilience. A hybrid architecture is needed, integrating the blockchain for immutable access control, the Post Quantum Cryptography (PQC) for quantum-proof security, and off-chain storage systems such as IPFS for scalability and privacy.

3.2 Research Objective

The primary goal of this research is to design, implement, and evaluate a secure, distributed data-sharing architecture that ensures the confidentiality, integrity, and availability of geospatial data in the presence of both classical and quantum adversaries. The specific objectives of this research are as follows:

1. Assessment limitations: Assess existing geospatial data protection methods, in particular with regard to their vulnerability to emerging quantum threats, and identify the need for a robust security model to withstand future challenges.
2. Develop a hybrid encryption scheme combining the following concrete algorithms: a) AES-256-GCM for symmetric encryption of potentially large geospatial files and b) Kyber-512 (a lattice-based key encryption mechanism chosen by the NIST standardization process) to protect symmetric key exchange from quantum-capable adversaries.
3. Leverage Decentralized Storage: Use the Interplanetary File System (IPFS) (Benet, 2014) for decentralized off-chain encryption storage, avoiding the scalability and cost problems of block-based data storage.
4. Design Smart Contracts: Create smart contracts to facilitate a granular access control policy (e.g., granting, revoking,

verifying) for encrypted data, ensuring that only authorized users can request decryption keys or access metadata.

5. Evaluate System Effectiveness: Assess the efficiency, scalability, and security of the proposed system by analysing encryption and decryption latency, resistance to unauthorised access and quantum attacks, and practicality for real-world geospatial applications.

By achieving these goals, this research aims to contribute to a practical and expandable framework for the security of geospatial data in the post-quantum era, while respecting the principles of decentralised trust and privacy-preserving design.

4. Methodology

This research introduces a hybrid cryptographic architecture to secure geospatial data. The system combines post-quantum encryption, decentralized storage, and blockchain-based access control to enhance data protection. It comprises four key modules of hybrid encryption to secure data, decentralized storage for reliable data maintenance, smart contract-based access management to regulate user permissions, and a REST API for seamless integration and exposure of functionality. Each module is specifically designed to tackle the unique security and scalability challenges highlighted in previous sections.

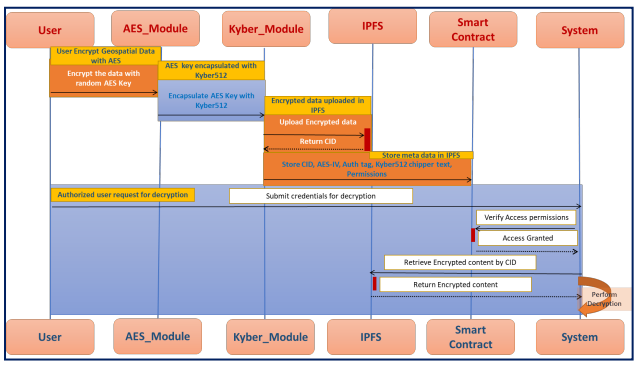

Figure 1: Methodology

The proposed geospatial data management and security architecture (see Figure 1) is composed of several key components: a client interface that allows users to upload geospatial data and manage access rights; a hybrid encryption engine that uses two-layer encryption using symmetric and quantum encryption methods; the Decentralized Storage Layer uses the InterPlanetary File System (IPFS) to securely store encrypted data outside the chain; the Blockchain Layer manages metadata, access protocols, and permissions through smart contracts to increase security and transparency; the Decryption and Authentication Module processes decryption requests and authentication using private keys.

This workflow involves encrypting geospatial data with a randomly generated AES key, encrypting the AES key using Kyber, and sending the encrypted data to IPFS with a unique content identifier (CID). The metadata, including CID and access rights, is stored in the Smart Contract. The authorized users can then provide the credentials to access, retrieve and decrypt the encrypted data. This architecture provides a robust framework for handling sensitive geo-spatial data with advanced encryption, decentralised storage, and management via the blockchain.

4.1 Hybrid Encryption Model Overview:

In order to ensure confidentiality and resilience against quantum computing threats, this system employs a hybrid encryption model that integrates two key components:

AES-GCM (Advanced Encryption Standard – Galois/Counter Mode): This algorithm is used to encrypt geo-spatial data. It is recognised for its speed and efficiency, while at the same time providing strong guarantees of confidentiality and integrity of the data processed.

Kyber: Employed for encapsulating the AES key, Kyber-512 is a lattice-based Key Encapsulation Mechanism standardized by NIST. This public-key scheme is specifically designed to be resistant to attacks by quantum computers that threaten conventional key exchange algorithms, such as those based on integer factorization or discrete logarithms, while enabling secure distribution of symmetric encryption keys.

The synergy of these two technologies ensures robust security; even if traditional encryption methods like RSA or ECC are compromised by quantum advances, the AES key remains secure unless the Kyber encryption is also compromised.

4.2 Decentralized Storage with IPFS

To address the high costs and storage constraints associated with storing encrypted data directly on-chain, this system leverages the Inter Planetary File System (IPFS) as its decentralized storage solution. IPFS offers several key advantages:

Content-addressed Storage: Data is accessed using cryptographic hashes, ensuring secure and unique identification of content.

Global File Sharing: Users can share and retrieve files based on their content rather than geographical location, enhancing accessibility.

The system effectively reduces blockchain overhead by recording only the Content Identifier (CID) and associated metadata on-chain, while storing the majority of the data off-chain. All encrypted data files are uploaded to IPFS, and only the CID is referenced in the blockchain contract. This approach facilitates efficient data retrieval, ensures immutability, and enables deduplication of stored files.

4.3 Blockchain-Based Access Control

In this schema, a smart contract developed in Solidity is deployed on a local Ethereum network, such as Ganache, to manage access control effectively. The primary functions of this smart contract include:

Recording Access Permissions: It facilitates granting and revoking access rights.

Logging Encrypted Data Metadata: The contract tracks essential metadata related to encrypted data, including the Content Identifier (CID), AES Initialization Vector (AES-IV), AES authentication tag, and Kyber ciphertext.

Verifying Access Rights: Before allowing data to be decrypted, the smart contract verifies the access rights of the requested user. Each authorised user is assigned a unique address to the wallet on the blockchain that serves as their access identifier. When requesting file decryption, the smart contract checks the requestor's address against its permission registry. Access is granted only if the requested rights are in possession of the user. The smart contract exposes several key features that are designed to simplify these processes.

5. Implementation and Evaluations

The proposed hybrid system combines AES-GCM encryption, Kyber post-quantum key encapsulation, decentralized IPFS storage, and smart contract-based access control through Ethereum. Our implementation is modular and extensible, specifically designed to tackle key challenges such as scalability, quantum security, and decentralized governance in the sharing of geospatial data. To facilitate user interaction with the system, a web-based User Interface has been developed.

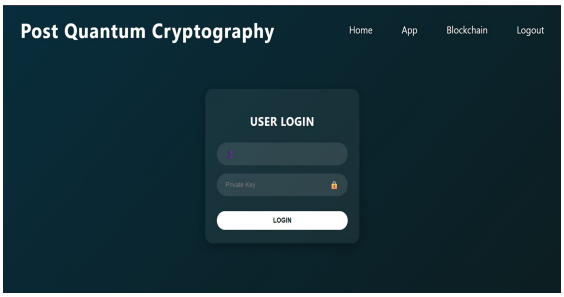

Figure 2: User Login Page

Figure 2 shows the login page, which enables secure user authentication before granting access to encryption, decryption, and blockchain operations. Figure 3 shows the main web page for users of the system, where key generation, file upload, and encryption can be triggered.

5.1 Key Generation Process

The key generation involves two main stages, corresponding to the symmetric and asymmetric components of the system.

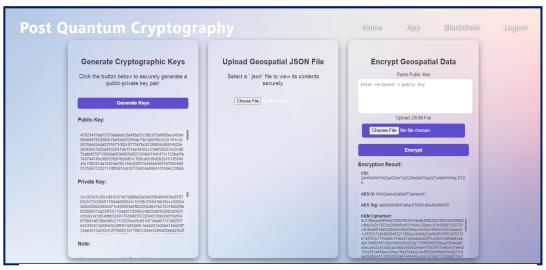

Figure 3: Key Generation and Encryption Page

AES-GCM Key Generation: AES (Advanced Encryption Standard) has been chosen for its high performance and wide acceptance in industrial and governmental applications. The system uses the AES-GCM (Galois/Counter Mode) encryption mode to provide authenticated encryption, which guarantees both confidentiality and integrity. The 256-bit symmetric key is generated by the Python Secrets module, which uses a cryptographically secure pseudo-random number generator (CSPRNG) to provide sufficient entropy and to withstand guessing attacks. For each session, a 12-byte Initialization Vector (IV) is generated in accordance with NIST guidelines for AES-GCM. This IV ensures that encrypting identical plaintexts produces unique ciphertexts, maintaining data integrity.

Kyber-512 Key Pair Generation: Kyber-512, a lattice-based key-encryption mechanism (KEM) from the Crystals suite, was selected by NIST in 2024 as part of its standardization efforts for quantum cryptography. Kyber512 is designed to provide an efficient key encapsulation with compact key sizes, while offering protection against quantum computer attacks. Generating keys is done with liboqs, a C-based library that bridges the gap between Python and C++. The key pair is build as follows: the public key (about 800 bytes) serves as a wrapper (encapsulation) for the AES encryption key. The private key (about 1.6 KB) allows authorized users to decrypt the AES key.

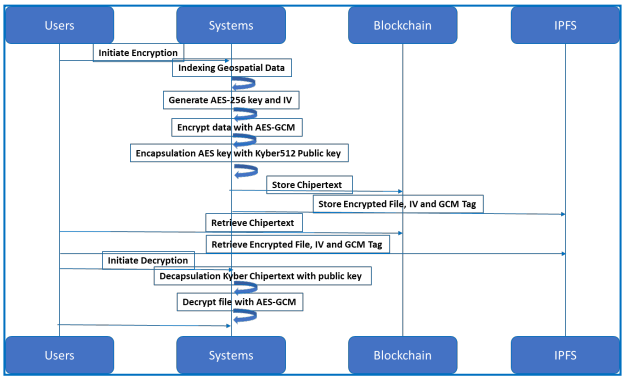

Figure 4: Encryption and Decryption of data

5.2 Encryption and Decryption Flow

Encryption Process: Geospatial datasets (such as JSON, GeoJSON, or TopoJSON) are first read and converted into byte streams. This byte stream is then encrypted with AES-GCM using a 256-bit symmetric key and a 12-bit initialization vector (IV). The AES key is then encapsulated with Kyber. The AES-encrypted byte stream is stored in the IPFS, while the Kyber-protected AES-key is stored on the blockchain. This hybrid encryption ensures that geospatial data remains confidential and is protected against both classical and quantum-enabled attacks.

Decryption Process: When an authenticated user requests decryption, he/she obtains the encryped file from the IPFS, and from the blockchain he/she obtains the authentication token and the encapsulated AES-key. Using the user’s private key, Kyber512 decodes the Kyber ciphertext to get the AES key. The encrypted file is then decrypted using the AES-GCM protocol and the decryption tag is used to verify the integrity of the decrypted data.

Figure 4 shows the encryption and decryption flow of the system, as described above. Note that in the figure the Kyber-protected AES-key which is stored on the blockchain is called “Ciphertext”.

5.3 Data Storage Using IPFS

In an age when high storage costs and network constraints challenge innovation, the interplanetary file system (IPFS) offers an elegant solution. This revolutionary, distributed, and content-based file storage system can empower users to unlock new possibilities. The storage process is as follows: Geospatial files are sent encrypted with AES through a local IPFS node or gateway, such as Infura, and the content identifier (CID) represents the file's SHA-256 hash. This CID is not just code; it is an important record embedded in the corresponding blockchain smart contract along with meaningful metadata.

Encrypted data linked to a CID can be accessed from any IPFS node worldwide. Since the CID is derived from the content, any tampering will be detected by a hash mismatch. IPFS improves traditional storage by decoupling it from the blockchain, enabling large-scale off-chain storage of files while ensuring on-chain validation.

This contribution has been peer-reviewed. The double-blind peer-review was conducted on the basis of the full paper.
https://doi.org/10.5194/isprs-annals-XI-4-2026-443-2026 | © Author(s) 2026. CC BY 4.0 License.

5.4 Access Control via Blockchain

Blockchain technology is leveraged to enforce access control through the use of smart contracts. In this work, Solidity-based smart contracts are deployed on a local instance of the Ethereum network using Hardhat. These smart contracts act as a decentralized access control layer, governing who is authorized to access encrypted geospatial data. A user-friendly web interface enables interaction with the system, allowing users to create and manage access permissions, as illustrated in Figure 5.

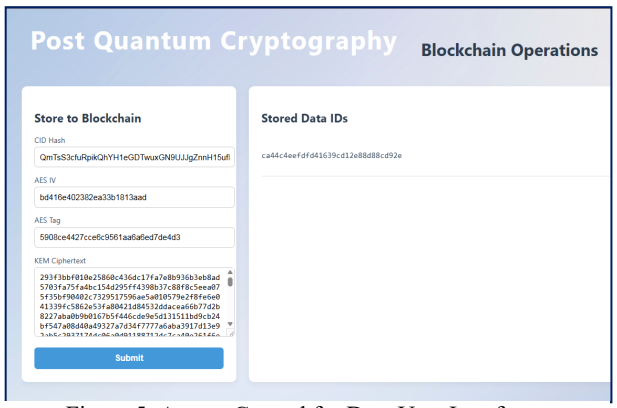

Figure 5: Access Control for Data User Interface

The smart contract is designed to securely manage metadata and enforce access policies. It provides core functionalities such as “storeMetadata(dataId, cid, iv, tag, kyberCiphertext)”, where:

- cid refers to the content identifier of the encrypted file stored in IPFS,
- iv and tag are parameters required for AES-GCM decryption, and
- kyberCiphertext contains the Kyber-512 encapsulated symmetric AES key.

In this architecture, the actual geospatial data are encrypted using AES-GCM and stored off-chain (e.g., in IPFS), while the blockchain stores only the associated metadata and encrypted key material. Access control is enforced by the smart contract, which ensures that only authorized users can retrieve the necessary decryption parameters (depicted in Figure 6).

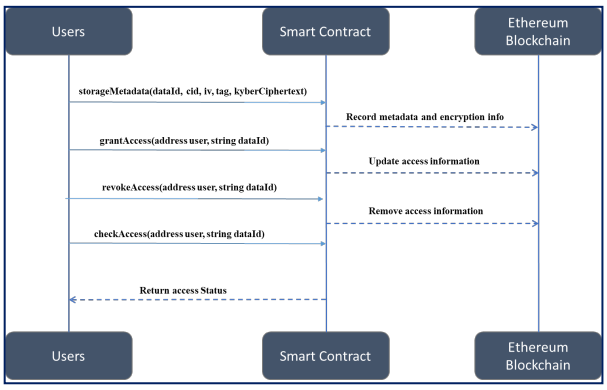

Figure 6: Access Control via Blockchain

When a user is granted access, the smart contract allows them to obtain the relevant metadata, including the Kyber-encrypted AES key. The user can then use their private key to decapsulate the symmetric key and decrypt the data. This approach ensures that:

- the data remain confidential (stored encrypted off-chain),
- the AES key is protected via post-quantum key encapsulation, and
- access decisions are transparent and tamper-resistant due to blockchain immutability.

Overall, the integration of blockchain and smart contracts provides a secure and decentralized mechanism for managing access to both encrypted files and their corresponding decryption keys, enabling a robust and scalable solution for secure geospatial data sharing.

5.5 Performance of Encryption and Decryption combined with IPFS

We investigated the performance of geospatial data encryption and decryption processes across varying file sizes of location and boundary layer data in JSON and GEOJSON formats. For evaluation purposes, datasets of sizes 0.1 MB, 1 MB, 5 MB, 50 MB, and 100 MB were used. All experiments were conducted on a standard desktop system equipped with an Intel Core i7 CPU and 16 GB RAM.

The reported execution times represent the total processing time of the proposed pipeline. Specifically, the measured time includes (i) AES-GCM encryption, (ii) Kyber-512 key encapsulation, and (iii) the time required to upload the encrypted data to IPFS. Therefore, the results reflect end-to-end system performance rather than isolated cryptographic operation costs.

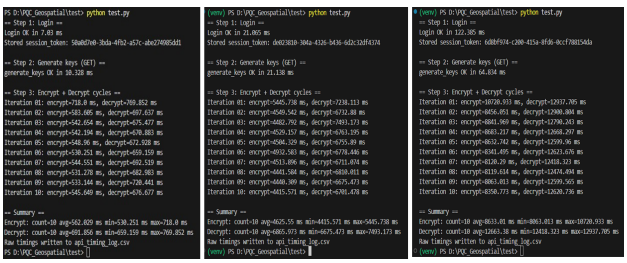

Figure 7: Testing of the various Data Size of the 5MB, 50MB and 100MB

Table 1: Overall Encryption and Decryption Time of AES-GCM and Kyber-512 for different File Sizes

File Size (MB)	Encryption Time (ms)	Standard Deviation (σ)	Decryption Time (ms)	Standard Deviation (σ)
0.1	159	32.36	2.5	0.16
1	227	52.89	144	7.63
5	562	9.00	691	11.00
50	4625	307.0	6865	259.0
100	8633	751.8	12663	142.6

Figure 7 shows illustrative CLI output from our prototype. Table 1 shows that overall encryption and decryption time increases with data size, reflecting the cumulative cost of AES-GCM encryption/decryption, Kyber-512 key encapsulation/decapsulation, and data upload/download to/from

This contribution has been peer-reviewed. The double-blind peer-review was conducted on the basis of the full paper.
https://doi.org/10.5194/isprs-annals-XI-4-2026-443-2026 | © Author(s) 2026. CC BY 4.0 License.

IPFS. The observed trend indicates a proportional relationship between file size and total processing time across the pipeline. These results demonstrate the general scalability of the integrated approach in handling varying geospatial data volumes within an end-to-end processing framework. Overall, these observations highlight the feasibility of integrating encryption, post-quantum key encapsulation, and decentralized storage into a unified pipeline for secure geospatial data processing.

5.6 Access Control and Security Validation

The access control logic was validated through simulated interactions, where authorized users successfully retrieved and decrypted data. Unauthorized users faced Smart Contract refusals, highlighting the system's functional access control and effectiveness in maintaining data security.

Table 2 provides an overview of the security properties of the proposed system, covering common threat scenarios. The results highlight its resilience to interception, tampering, and unauthorised access. In addition, the implementation of Kyber-512 encryption provides strong, quantum-proof protection and strengthens the system's overall security framework. The evaluation revealed that the proposed system has practical applicability for sharing sensitive geospatial data in a decentralized, quantum-secure environment.

Table 2: Security Properties of the Proposed System

Threat Scenario	Outcome
Man-in-the-Middle attack on key exchange	Protected via Kyber-512 post-quantum key encapsulation
File tampering (IPFS data swap)	Detected via a hash mismatch in CID
Unauthorized access attempt	Denied via checkAccess() smart contract function

6. Results and Discussion

The system addresses the challenges of securing sensitive geospatial data in a post-quantum, decentralized environment by connecting technical choices to research objectives and discussions.

6.1 Benefits of the proposed system

Compared with existing geospatial data security models, the integrated system offers several significant advantages.

- The Kyber-512 key encapsulation mechanism (KEM), standardised by NIST and based on lattice cryptography, offers a high resilience to quantum attacks (NIST, 2025). This makes it a safe choice in the post-quantum world, as opposed to the legacy systems that use RSA or ECC.
- The system uses the Inter Planetary File System (IPFS) for data storage, which helps to avoid the high costs and size constraints of chain storage. The IPFS system ensures data integrity by addressing content and is integrated seamlessly with Smart Contract Systems.
- Ethereum smart contracts manage fine-grained and transparent access control, eliminating the need for centralized access controllers and enabling users to independently verify access in a trusted environment. Access requests shall be traceable and auditable.
- The architecture is designed to be modular, allowing each component—encryption, storage, and smart contract—to be upgraded or replaced independently. This flexibility enables the system to adapt to future cryptographic advancements or platform transitions.

6.2 Limitations of the Current System

Key Management Complexity Although Kyber provides strong security, the safe storage and distribution of private keys remains a challenge. If the user loses their private key, they will not be able to decrypt any data. Future work should focus on exploring key backup solutions and integrating with secure hardware, such as hardware security modules (HSMs).
IPFS Availability: IPFS relies on content bundling to ensure data persistence. If the data is not actively pinned or accessed, it may be collected as trash. Without a permanent pinning strategy, the availability of data may degrade over time (IPFS, 2025).
Gas Costs and Performance Trade-offs: Although metadata storage is minimised, the interaction with smart contracts still generates Ethereum gas costs, especially during batch operations or large scale deployment. In addition, Kyber512 introduces a slight performance overhead compared to elliptic curve cryptography (ECC) due to the complexity of lattice-based computing.

7. Conclusion and Future Work

This section highlights the findings of the research, showing the contributions, impacts and challenges of the proposed scheme. It also provides a vision for future efforts to increase security, scalability and usability in geospatial data management.

7.1 Conclusion:

Rapid growth in the use of geospatial data in areas such as urban planning and disaster response has created a need for secure and scalable data protection. This paper addresses this need by developing a modular system that integrates the use of blockchain technology, quantum-blockchain (QBC) and decentralised storage for secure sharing and control of geo-spatial data. Key contributions of this research include:

Hybrid Encryption Model: A hybrid encryption model has been implemented using AES-GCM for fast, authenticated geospatial file encryption, complemented by Kyber-512, a lattice-based key encapsulation standardised by NIST. This combination guarantees both high performance and strong future-proof security.
Decentralized Storage: The system uses the InterPlanetary File System (IPFS) to store encrypted data off-chain. This approach allows scalable and distributed access, while avoiding the costs of storing the blockchains.
Access Control Mechanism: A smart contract access control system has been developed and is being deployed on the private Ethereum network. This mechanism allows fine-grained control of permissions (granting, revoking, verifying) via wallet-based identity.
Performance Evaluation: The integrated system was evaluated using test datasets and simulated environments, demonstrating its overall performance and scalability.

Overall, this architecture has combined addressing key research objectives: confidentiality, integrity, decentralised management, and quantum resilience in protecting geospatial data.

7.2 Broader Impact

This paper shows how integrating emerging cryptographic techniques with decentralised infrastructure can effectively address data privacy and data integrity challenges in practice.

The key message is that sensitive geospatial information may not depend on centralized cloud providers for security, and that post-quantum cryptography has moved from a theoretical concern to a practical requirement to ensure long-term security in data management.

7.3 Limitations

The system discussed in this paper, while successful, does face several notable limitations:

Key Management: The Kyber512 mechanism provides a high level of security, but managing private keys is risky. Losing the private key permanently blocks access to the data. Secure enclaves or decentralised identity (DID) systems could be integrated to improve this.
Storage Availability in IPFS: The InterPlanetary File System (IPFS) provides a decentralized file store, but its reliance on a file-access lock may be problematic. Without a robust file pinning solution, such as Filecoin or IPFS, file lifetime and availability may be at risk.
Gas Costs and Scalability: Smart contract use may result in fluctuating costs that vary with the underlying blockchain network. In particular, the use of public Ethereum networks may incur high costs that are prohibitive for applications that require frequent access to and updates of metadata.

7.4 Future Work

This work has opened several promising avenues for future research and development:

Integration with Post-Quantum Digital Signatures: The system currently uses Kyber-512 to encapsulate the keys, but it does not support post-quantum digital signatures. Future improvements could include NIST-standard signatures, such as Dilithium or SPHINCS+, for secure authentication and digital signatures.
Decentralized Identity and Verifiable Credentials: Future systems could use decentralized identity (DID) and verifiable credentials (VC) to improve access control. Frameworks such as W3C DID and Hyperledger Ares allow selective disclosure of access rights without revealing full identities.
Enhanced File Availability via IPFS Pinning Services: To ensure the continued availability of IPFS data, use pinning services such as Pinata, IPFS clusters, or filecoin integration, which provide economic incentives to store data.
Scalability Testing on Public Blockchain Networks: This paper used Ghanach's work and Hardhat to simulate, but future research may include deploying smart contracts on public blockchains like Polygon, Optimism, and ZkVM. This would enable cost-benefit and scalability assessments in real-world settings. Future work should include performance benchmarking, scalability testing with large geospatial datasets (e.g., high-resolution raster or vector databases), and evaluation under distributed blockchain environments to validate the scalability claims.
Homomorphic Encryption or Zero-Knowledge Proofs (ZKPs): Incorporating homomorphic encryption or zero-knowledge proofs can enable secure geospatial calculations and access verification without exposing sensitive data.
Incorporate other Geospatial file formats: Future work could also focus on extending the framework to support encryption and decoding of other geospatial data formats, such as shape files, Satellite images, and geodatabases. This improvement will improve interoperability with standard GIS systems and allow for the secure management of a variety of spatial data sets. Effective cryptographic mechanisms to handle large spatial file structures and still maintain performance will also be explored.

These directions promise to enhance the system's capacity and security while adapting to new standards and technologies. The research introduces an innovative architecture for the secure and efficient sharing of geo-spatial data. It emphasises cryptographic integrity, decentralisation and resilience to quantum attacks. This framework hence provides a solid basis for the next generation Geographic Information Systems (GIS).

Acknowledgements

This work is an outcome of the project "Datasecurity4icity", a subproject of the project "ICity: Intelligent city" (https://www.hft-stuttgart.com/research/projects/i-city)". We extend our gratitude for the funding received through the FH-Impuls program under the number 13FH9E04IA by the German Federal Ministry of Education and Research (BMBF).

References

Antonopoulos, A. M. (2017). Mastering Bitcoin: Unlocking digital cryptocurrencies (2nd ed.). O’Reilly Media.

Benet, J. (2014). *IPFS – Content Addressed, Versioned, P2P File System (Draft 3).* arXiv preprint arXiv:1407.3561. https://arxiv.org/abs/1407.3561.

Elwood, S., Leszczynski, A. (2018). Feminist digital geographies. Gender, Place & Culture, 25(5), 629–644. https://doi.org/10.1080/0966369X.2018.1465396.

Goodchild, M. F. (1992). Geographical information science. International Journal of Geographical Information Systems, 6(1), 31–45. https://doi.org/10.1080/02693799208901893

InterPlanetary File System (IPFS). (2025). Persistence and pinning. Retrieved July 22, 2025, from https://docs.ipfs.tech/concepts/persistence/.

National Institute of Standards and Technology (NIST). (2007). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (NIST Special Publication 800-38D). https://doi.org/10.6028/NIST.SP.800-38D.

National Institute of Standards and Technology (NIST). (2025). Post-Quantum Cryptography Standardization Project. Retrieved July 22, 2025, from https://csrc.nist.gov/projects/post-quantum-cryptography.

Pandeni Paavo, J.; Rodríguez-Puentes, R.; Chigbu, U.E. Practicality of Blockchain Technology for Land Registration: A Namibian Case Study. Land 2025, 14(8), 1626. https://doi.org/10.3390/land14081626

Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E. (1996). Role-based access control models. Computer, 29(2), pp. 38–47. https://doi.org/10.1109/2.485845

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700.

Udodiri, A.; Ajakwe, S.; Lee, J.M.; Kim, D.-S. Internet-of-Things-Blockchain Integration in Environmental Pollution Monitoring Data Management: Trends and Techniques. International Journal of Environmental Science and Technology 2025, 22. https://doi.org/10.1007/s13762-025-06615-x