Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

SMSDI: Secure Multiservice Spatial Data Infrastructure using Public Key Cryptography

Nikhil Khandare[*,1],Valmik Nikam[2]

[1]Assistant Professor; nbk0918@gmail.com, [0000-0002-8070-1717]

[2]Associate Professor; vbnikam@it.vjti.ac.in

[1,2] Veermata Jijabai Technological Institute, Mumbai, India

*Correspondence: nbk0918@gmail.com

Article History:

Received: *28-10-2024*

Revised:*12-11-2024*

Accepted:*19-12-2024*

Abstract:

With the aim of making spatial data readily available to people, enterprises, and governments for successful regional, state, and national decision-making, countries are focused on building spatial data infrastructure that can provide reliable spatiotemporal data. Nonetheless, numerous issues need to be dealt with before, during, and after the creation of spatial data infrastructure.Accuracy, dealing with big data, analysis of large spatial data, time to fetch data, privacy protection are different SDI issues. Huge work has been undertaken into the study and precision of spatial data, but relatively little attention is paid to the security of spatial data infrastructure. So this paper proposes an architecture for secure SDI based on elliptic curve cryptography to address this problem.Security is implemented at different levels of SDI, incorporating different features to improve SDI security. Such features include a modern authentication algorithm, secure calls to service, safe data transfer, and secure data storage in the database. The Secure-SDI proposed is safe against all well-known attacks, and proof of concept is also provided in security analysis

Keywords: Spatial Data Infrastructure; Security; Elliptic Curve Cryptography; Public Key Cryptography; authentication; Diffie-Hellman key exchange; Geo-Portal, Spatial Database

1. Introduction

Spatial data infrastructure links nodes at different universities, organizations, and other entities that have spatial data or that need it. Spatial data infrastructure has different elements, such as spatial data, metadata, human capital, standards, technological resources, communication platforms, networks, policies, and institutional arrangements, to name only a few[1][2].Policies and regulations are applied from an open geospatial consortium [3], also Web Mapping Service (WMS), Web File Service (WFS), and Web catalog service (WCS) are used to get data from the nodes [4]. When this huge spatial data goes online there is always insecurity regarding the purpose for which this data will be used[5]. A review of Geospatial One-Stop (GOS) was done in[6], which is a single SDI developed by the US government for spatial data. The need for securing spatial data (meteorological and climatic data) was highlighted in[7]. Spatial data e-Infrastructure was proposed in [8] to provide secure access to geospatial data, few examples were given, and new architecture was also proposed for secure access to spatial data. Privacy and confidentiality are the policies that hinder the availability of spatial data[9], thus these policies should be addressed very carefully and should be taken care of while designing SDI. The need for privacy, confidentiality, and secure sharing of spatial data are key points that need to be considered while designing spatial data infrastructure. On

the same grounds, a way for secure sharing of spatial data was given in [12], the author used the methodology of public-key cryptography for secure sharing of geographical data.

This paper is organized as follows, Section 2 addresses similar work on spatial data infrastructure and security, section 3 addresses proposed secured spatial data infrastructure and different modules within the proposed framework. Detailed security analysis of the proposed work is done in section 4. The findings of the research are given in section 5 and section 6 concludes the paper.

2. Related Work on Spatial Data Infrastructure and Security

2.1 Spatial Data infrastructure

The general architecture of spatial data infrastructure is discussed here in this section. Here the architecture is divided into layers, mainly three main layers are discussed, namely the geoportal layer, network layer, and database layer.

Geo-Portal Layer

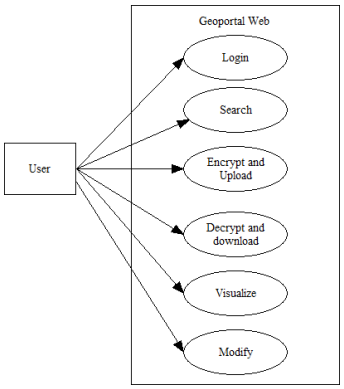

Figure 1: Geoportal Layer of Spatial data infrastructure

Figure 1 shows the geo-portal layer, it is showing what operation the user can perform on the geo-portal layer. Users interact with spatial data infrastructure through its geo-portal[13][14]. There are many operations that users can perform on spatial data infrastructure. Some major operations include login into SDI, search geographical data, encrypt and upload geographic data, decrypt and download, visualize, edit metadata.

Network Layer

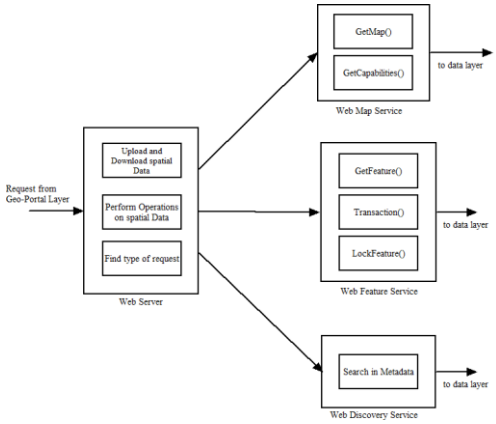

Figure 2: Network layer of SDI

Figure 2 shows the network layer of SDI, when the user gives some requests on the geo-portal layer, it is forwarded to the network layer. The request then goes to a web server (which finds out the type of the request), where users can upload, download spatial data, or perform some operations on spatial data. The web server has various services in it like WMS (web mapping service), WFS (web feature service), WDS (web discovery service) to name the few [15][16]. Through these services, data is accessed, modified from the spatial database. Consider an example wherein the client wants to get a map of LULC(land use land cover) of Mumbai city in India. The user's request will be forwarded to WMS, where it will use the function getmap(). Requests from the network layer are then forwarded to the database layer.

Database Layer

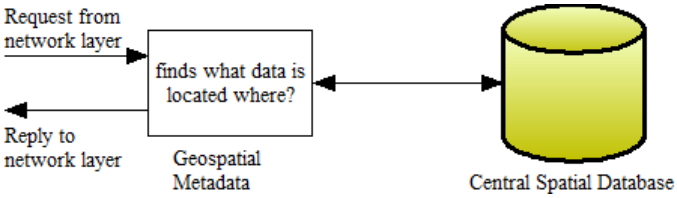

Figure 3: Database layer of SDI

Figure 3 shows the database layer of SDI. The request from the network layer comes to the database layer [17][18], then metadata is searched and data from the spatial database is obtained. A reply is given to the network layer and which is then forwarded to the user through the geo-portal layer.

The spatial data analytics infrastructure was designed by the "Brazilian National Institute of Space Research" which was named 'TerraBrasilis'. Along with spatial data infrastructure, spatial data analysis infrastructure was also developed which uses complex algorithms for analysis. To speed up the execution of SDI and processes, microservice architecture was used [22]. A basic study of spatial data infrastructure was done in [23], NSDI developed by the United States of America, Canada, and Europe was studied, and the benefits of spatial data infrastructure, as well as its components, were studied. Strategic, financial, and other benefits were given. Development in SDI in Europe was studied and the trend towards the development of open spatial data infrastructure was studied in [24], with the understanding that spatial data is useful not only to the government but also for business and private sector, people have started to share and use spatial data. Gap analysis of spatial data infrastructures in Africa was done in [25], this was done based on 14 key indicators of evaluating SDI. The score of African SDI was lower and the need to improve statistical information was highlighted for most of the African countries.

A case study was done to mark Spanish heritage in spatial data infrastructure as a protected site, cultural heritage development schema developed by IDEE, cultural heritage was marked as a special kind of protected site, and some difficulties involved were also given [26]. Development of SDI was highlighted as an inseparable part of globalization, as globalization occurs there comes a need of better SDI (local, regional, and national), Also the development of the real estate market was shown and how ownership documentation system (cadastral system) has evolved was shown [27], thus with the evolution of the cadastral system over time, there comes the need of SDI. With the vision of getting reliable information over the Arctic Ocean, Arctic SDI was started, it was based on the cooperation of various national organizations, it is expected that this SDI will give huge spatial information (which will be used for many purposes) over the Arctic [28]. Many researchers are working on climate change research; however, the availability of climate spatial data is a problem for

most researchers. With the aim of availability and cheap climate spatial data, Climate spatial data infrastructure was developed for Nepal. Climate SDI was proposed and geo-portal was designed for climate data to be easily available at cheaper rates [29]. Local spatial data infrastructure was evaluated for the Seoul Metropolitan Government and parameters for the development of this LSDI were proposed which include analysis of cost-benefit, manpower, systematic development of the LSDI plan to name a few[30].

A Survey of NSDI of countries in Africa was done in [31], the basis for this study was that countries having good NSDI will achieve greater developments in the future. Thus the evaluation of 12 countries for the readiness of NSDI was done and they were graded from 0 to 1, in which the score of Senegal was 0.69(highest) and Zimbabwe was 0.33(lowest). Taking into consideration real estate ownership and registration, a cadastral agency in Kosovo was working on developing NSDI for Kosovo, this is believed to change the way that spatial data is shared between users, the design and implementation of NSDI were completely following INSPIRE directives[32]. A study related to how INSPIRE has changed the way spatial data was made available to the public was done in [33], above framework has given standards for technology as well as policies, common ground was set using this standard. The formal model given by the International Cartographic Association was used by Cemig to develop SDI for discovery and sharing of spatial data for its employees and companies who are partners with Cemig, this SDI was called SDI-Cemig[34]. To protect the quality and security of spatial data, a new access method was proposed, the concept of centralized searching for spatial data was removed and a distributed model was proposed, Nigerian NSDI was taken as a case study [35].

GIS is widely being used for groundwater discovery on the similar grounds, Concept and prototype of web services were given for various web services for groundwater in [36], all the web services were complying with OGC standards, Climate data and groundwater data was taken for this research. Spatial data infrastructure for environmental noise data was developed and principles of spatial data management were given in [37], these principles can be applied to understand environment noise. The methodology for developing marine SDI was given in [38], multi-criteria decision making was used for priority ranking of various classes of data, and thus marine SDI development plan was given. A study on the usefulness of SDI for the land survey was done in [39], instead of using cartographic maps or toposheets, Geo-portals were used as a source of data, Impact of SDI on user organization performance was studied. Multi-criteria decision making was used for assessing the performance of SDI, Polish-SDI was used for reference, and research included indicators and multi-criteria method [40]. For SDI, assessment categories were defined and scores for those categories were calculated.

Comparison between key elements of indoor location-based service and SDI was done in [41], the two frameworks were compared for key elements like people, data, policies, and technology. The authors also gave similarities and dissimilarities, the authors gave few areas where we can both can be benefitted by sharing experiences. With a large number of devices connected (called smart devices) in the IoT system, the need for security and privacy in spatial as well as other data was highlighted and a secure access control protocol was proposed based on attribute-based encryption and controlling communication[42]. In SDI most of the time while generating rainfall maps or temperature maps we need data from each location to come to the correct result. However, lack of data has always been a problem in SDI, there isa need to predict the data that is missing. To predict missing data correctly, a new interpolation technique called semantic kriging was proposed in [43], experimentation was done with temperature data for interpolating the data of four major cities in the

country. In SDI we need maps of urbanization; these can be done using spatial data of urban areas. We can do some analytics on this data to get how much growth has occurred in the past 'n' years in the given city. One such effort has been put in [44], where urban data from Delhi (India) was monitored; the Shannon entropy index was used to depict the outgrowth of sprawl areas. Detecting outliers in spatial data can be difficult sometimes, but if detected, it may lead to the discovery of useful data. A fast algorithm for detecting outliers was proposed in [45], the performance of the system was evaluated using different data clustering services.

In case of disasters like Amphan which has recently hit the Indian states of Odisha and West Bengal, evacuating people is a big challenge to the state and central government. An efficient algorithm for evacuation planning was designed in [46], in experimentation, it showed significant improvement over capacity-constrained route planner. To enable citizens to gather information about the environmental factors like temperature and quality of air, spatial data infrastructure was proposed called 'smart emission'[47], various areas in which above SDI can give significant improvement were also given. Many organizations are facing the problem of getting spatial data and reusing it, to solve this problem SDI for earth observation data is proposed in [48]. Challenges in the design of coastal spatial data infrastructure were highlighted in [49], challenges faced by people from various countries were given. Data analysis was an important part after the availability of data, on similar grounds, Data analysis of cadastral data in polish spatial data infrastructure was done in [50], the author had done the survey for many years about cadastral data in SDI and reached to the conclusion that the condition of SDI was far from perfect till date.

Various architectural models for SDI were given and a geospatial one-stop portal was also given for accessing, modifying, and sharing of spatial data, Also. Open geospatial standards were given and SDI was defined at various levels like regional and national [51]. Model for spatial data infrastructure for rural areas in Turkey was developed in [52], a given model was compiled with INSPIRE directives and also with Turkish spatial data infrastructure; especially for all kinds of land use, the use of sensors was proposed. Apart from infrastructure for spatial data, there is a need for analysis of spatial data, this analysis should be done by using more advanced techniques and GIS software, the way deep learning can be used for spatial data analysis and remote sensing was given in [53].

2.2 Security: Public Key Cryptography

In public-key cryptography, keys used for encryption and decryption are different, each user has two keys (e,d), where "e" is the public key (called encryption key) and "d" is the private key (decryption key). Here we use elliptic curve cryptography (ECC)[19] (which is public-key cryptography) for securing spatial data infrastructure. ECC has become a crucial part of developing a secure cryptosystem. The security of ECC is dependent on the hardness or difficulty of DLP (discrete logarithm problem)[20].

Diffie-Hellman key exchange protocol was proposed by Diffie&Hellman[10], this protocol when combined with elliptic curve cryptography gives a more secure key exchange algorithm [21]. Details of this key exchange algorithm are given below.

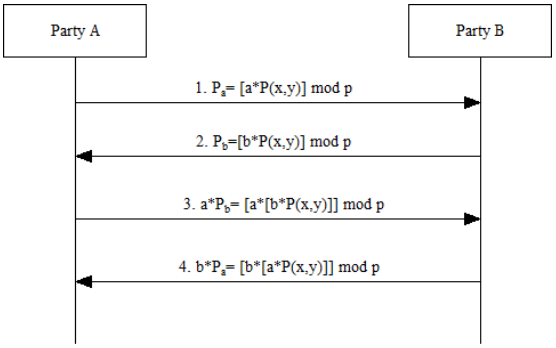

Figure 4: Elliptic curve Diffie-Hellman Key exchange

User A and B agree on a particular point P which is group generator, 'a' is the secret key of A, 'b' is the secret key of B. Using this algorithm both parties A and B can agree on the shared secret key over an insecure channel (without actually sharing key) as shown in figure 4.

1. User A calculates P_a=a*P and sends to B, User B calculates P_b=b*P and sends to A
2. Now user A has P_b and user B has P_b.

a. User A calculates a*P_b and sends to B

b. User B calculates b*P_a and sends to A

3. Now both parties have shared secret key a*b*P=b*a*P=a*P_b=b*P_a

In generalized El-Gamal public key cryptosystem over elliptic curve points, there is group G, and an operation '.' defined in the group. Let 'α' be the generator of this group, 'a' is chosen such that 0 <= a <= |G|- 2 (here 'a' is private key). $\beta = \alpha^a$, finding a is difficult due to the discrete log problem. Here the public key is (G, α, β) and 'a' is the private key. Encryption of message "x" in this scheme is defined as

1. Alice chooses random number 'k' such that 'k' is between 0 and |G|-2
2. Alice encrypts using Bob's public key $Ee_b(x,k)=(y_1,y_2)$, where $y_1=\alpha^k$ mod p and $y_2= x*\beta^k$ mod p.
3. Bob decrypts ciphertext and gets back message as $x=y_2*((y_1)^a)^{-1}$.

Following are the mathematical hard problems on which security of ECC relies

1. *Elliptic curve discrete logarithm problem (ECDLP):* Given two elements A and B $\in F_q$,then it is impossible to find an integer n such that B=nA, where A is a primitive element of the group.

2. *Elliptic curve factorization problem (ECFP):* Given two elements A and B $\in F_q$,then it is impossible to find an integer p and q such that, B=k*A + l*A, where k and l $\in F_q$, and k*A and l*A are impossible to find in polynomial time.

3. *Elliptic curve computational Diffie Hellman problem (ECCDHP):*Given (A, k*A, l*A) $\in F_q$, then it is impossible to find k*l*A in polynomial time algorithm.

4. *Elliptic curve decision Diffie Hellman problem (ECDDHP):* Given (A,k*A,l*A,m*A) $\in F_q$, for some integer k,l,m .It is impossible to decide m*A=k*l*A, i.e. to decide m=k*l or not.

In literature lots of work is done on location-based services (LBS), the security of LBS, and spatial data infrastructure, however, very little attention has been paid to the security aspect of spatial data

infrastructure (to the best of the author's knowledge). This negligence inthe security of spatial data infrastructure has been the greatest motivation for this paper. Question like

1. Who is getting spatial data from spatial databases?
2. Is the communication between entities in spatial data infrastructure is secure?
3. Can some external person attack SDI and get data from SDI?

Needs to be answered. To address these questions, this paper deals with enhancing the security of spatial data infrastructure by using public-key cryptography (PKC). To answer question 1, a secure authentication algorithm is proposed in section 3.4. To answer question 2,"secure service calls"are proposed in section 3.5. To answer question 6,the security analysis of SDI is done in section 4.

3. Proposed Work

In this section, secure SDI has been proposed wherein architecture, a flowchart of secure SDI is discussed. Also,a secure authentication protocol is proposed. Various services that will be given in SDI are listed and the mechanism to secure service calls is discussed. Each event of uploading, downloading, modifying, and querying done by an authenticated user is captured.

3.1 Architecture of Secure SDI

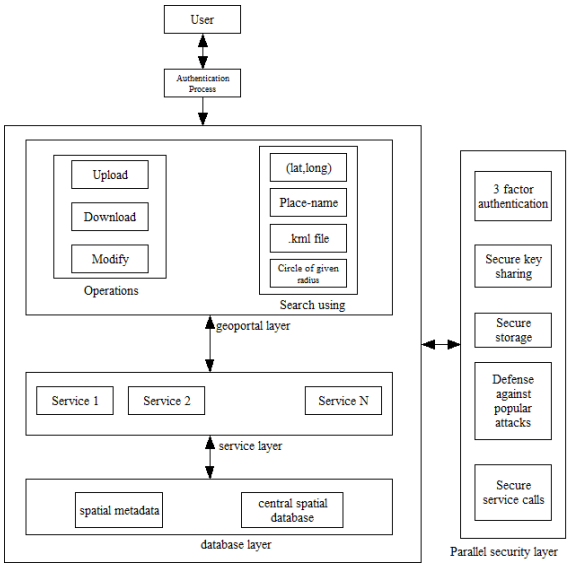

Figure 5: Architecture of secure spatial data infrastructure

`Figure 5 shows the architecture of the proposed secure SDI. It shows various layers in secure SDI, various layers are Geo-Portal layer, Service Layer, Database Layer, and Security Layer. User can get geospatial data by searching on geo-portal by giving input as

1. Latitude longitude details
2. Place-Name
3. KML file
4. A circle of radius "x" kilometers considering the given (lat, long) as a center.

When the spatial data becomes available to the user, the user can perform the various function on that data which include,

1. Upload
2. Download
3. Modify
4. Visualize

From the geo-portal layer, the request then comes to the service layer, where various services can be accessed by the user. These services are accessed for the particular location, which is given as input by the user in the geo-portal. Once the user decides which service he wants to use, data regarding that service and location is accessed from the database. Here Postgres is used for storing spatial data; database servers are made available online.

In this spatial data infrastructure, a parallel security layer is added to add security at each layer. This security layer is taking care that

1. User is authenticated to System
2. Secure service calls are made between different layer
3. Data is stored in a database securely
4. The system is secure against popular attacks
5. Key is shared securely between parties

How this security will be achieved will be discussed in detail in sections 3.4 and 3.5.

3.2 Access flow of Secure SDI

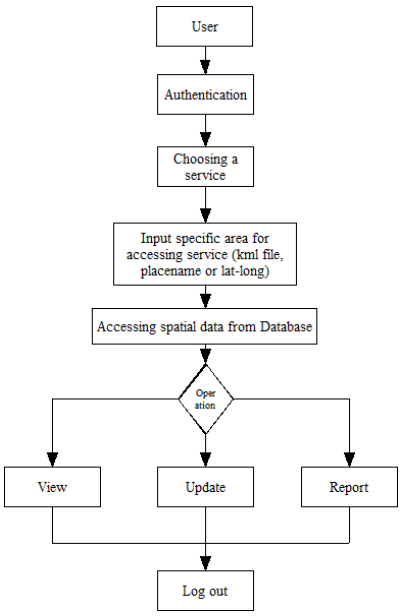

Figure 6: Access flow of secure SDI

Figure 6 shows the access flow of operation in secure SDI, User will choose the service of secure SDI and the User will choose the area for which he wants the service. Users enter location information like KML file, place-name, and latitude-longitude information. Based on the information, spatial data is accessed from a spatial database. Users can view, update, query, and

visualize map-data, attribute-data, and metadata. For each transaction (viewing, updating, and reporting). Finally, the user will log out of the system.

3.3 Services in secure SDI

The following services are proposed in secure spatial data infrastructure, data analysis can be done on GIS software (ArcMap or QGIS), and analyzed data will be published on GIS web server which will be made available to users. For spatial data analysis, toposheets, data from satellites can be used. This can be georeferenced, digitized, and analysis can be done for what service is needed. This analyzed data can be used for visualization, decision making, disaster management, etc. There is no limit to what extent this data can be useful, data from SDI can be used in many ways. In this paper,the focus has been maintained on what services should be present in SSDI or NSDI. “How can these services be implemented?” Or “How the analysis can be done for a particular service?” can be an extension of this paper.

The following services are proposed in secure SDI,Land Use land Cover Map (LULC), Rainfall Map, Temperature Map, Industry Map, Ground Water level Map, School Map, Hospital Map. Road Map, Rail Map, Administrative Boundaries Map, Forest Map, Agriculture Map, Mineral Map, Fire Services Map, Police Stations Map, Public Toilets Map, and Disease Spread Map.

3.4 Authentication and Key Sharing

As per section 2.2 using the elliptic curve Diffie-Hellman Key exchange is used to share the keys between parties. The authentication protocol used for authenticating parties to each other is shown in figure 7. Notations used in authentication protocol are given here

e_U: Public key of user or encryption key of user

d_U: Private key of user

e_S: Public key of system

d_S: Private key of system

Ee_U: encryption using User’s public key

Dd_U: decryption using User’s private key

Ee_S: encryption using system public key

Dd_S: decryption using system’s private key

Ed_U:encryption using user’s private key

De_U: decryption using users public key

Ed_S:encryption using system’s private key

Ds_U:Decryption using system’s public key

ID_U: identity of user

ID_S: identity of system

R(): request

C: Challenge

B_U: biometric details of user

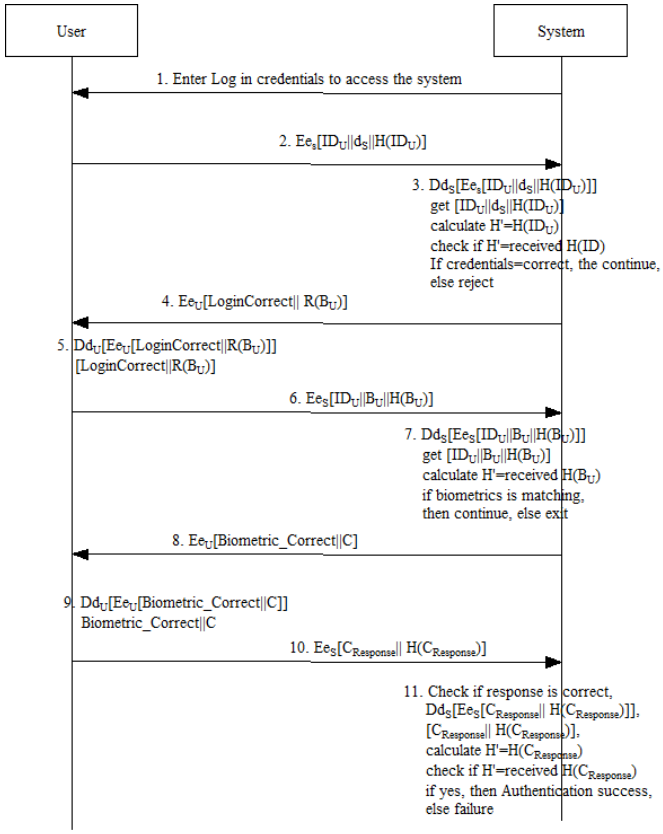

Figure 7: Proposed secure authentication protocol for SDI

1. User is asked to enter (username, password) to login

2. User sends Ee_S $[ID_U||d_S||H(ID_U)]$i.e Identity, key, and hash of identity. Encryption is done using public key of system, so that only system can decrypt it using its own private key.

3. Based on the credentials given by the user, the System will decide whether login is success or failure.

a. System checks if the response is correct.

b. System Decrypts {Encrypted (Public key, Private Key, and Hash of the message)}.

c. The system gets (Public key, Private Key, and Hash of the message).

d. System calculates hash of identity H'(ID).

e. Check if the two hashes are the same H'(ID)==H(ID), which means the integrity of the message is protected.

f. If all credentials are correct, then the user is given access to the system else the user is denied access.

4. The system will give the success message that login is correct (this success message is encrypted) and ask for biometric from the user. System will send $Ee_U[LoginCorrect||\ R(B_U)]$. Note that this message is encrypted using public key of user, which implies, only user can decrypt using his/her private key.

5. An encrypted message is sent to the user mentioning that the login attempt is successful. This message is then decrypted and the User gets a “login success” message and also gets the request for giving biometric.

6. User sends encrypted (identity, biometric, Hash(biometric)).i.e$Ee_S[ID_U||B_U||H(B_U)]$

7. Based on biometric details given by the user, the system gives success and failure message

a. System decrypts encrypted (identity, biometric, Hash(biometric)).

b. Calculates hash of biometric i.e. H’(biometric)

c. Check of H’(biometric)==H(biometric) i.e. received biometric

d. If both the biometricsarethe same, then biometric is a success.

8. The system gives an encrypted “biometric correct” message and gives the user a challenge.

9. The user decrypts the message received in step 8 and gets a biometric success/failure message, the user also gets the challenge to solve.

10. The user sends an encrypted response to the challenge and hash of response to ensure that the response message does not tamper. i.e$Ee_S[C_{Response}|| H(C_{Response})]$

11. Based on the response that was given by the user system completes the authentication process and give authentication success or failure message

a. System decrypts encrypted message $Dd_S[Ee_S[C_{Response}|| H(C_{Response})]]$and gets $[C_{Response}|| H(C_{Response})]$

b. The system calculates the hash of response i.e.H’($C_{Response}$).

c. Check if H'=received H($C_{Response}$), i.e. if both hash matches then the response message was not altered. Then the system declares authentication success.

3.5 Secure Service Calls

Service calls in SDI are secured using elliptic curve cryptography, the following two modules discuss how the service calls from geo-portal to the service layer and service to database layer are secured.

3.5.1 Geo-Portal and Service Layer

Notations used in this communication are,

E(): Encryption,

D(): Decryption,

(e_S,d_S): (Public, Private) key of service layer,

(e_G,d_G): (Public, Private) key of geoportal layer

ID_U: Identity of user,

K= (serviceID||Location||resolution)

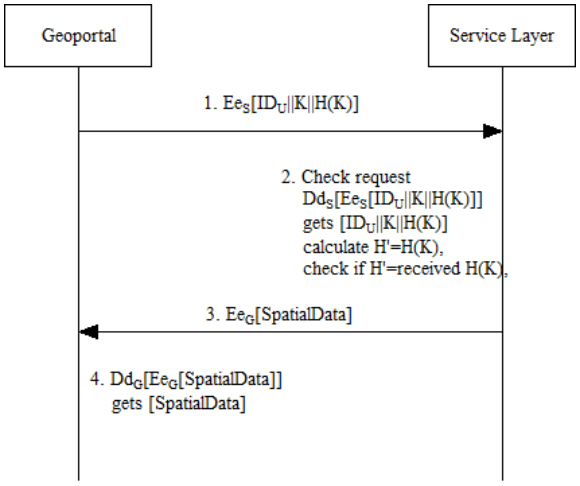

Figure 8: Secure service calls between Geo-Portal and Service Layer

Communication between the geo-portal and the service layer is shown here in figure 8. A user requests some service to the service layer (service can be any service listed above in section 3.3). Here a user can give a key (K) to the service layer where "K" comprises (Service ID, Location, and Resolution).

Consider if ServiceID=1, then the user wants LULC (land use and land cover map) similarly the user can use different service IDs for different services mentioned in section 3.3.

Location can be specified by the user by using (latitude, longitude), Circle of the given radius around given (latitude, longitude), User can also give location using a KML file.

Presently, the proposed system has three different types of resolution, low resolution, medium resolution, and high resolution. Thus, the user has to specify any one of three resolutions.

Communication between Geo-portal and service layer in secure SDI is discussed below,

1. Geoportal sends (ID_U, K, Hash(K)) to the service layer. This request is sent in encrypted form. It sends $Ee_S[ID_U||K||H(K)]$

2. The service layer checks "if the request is correct".

a. Service layer decrypts the request$Dd_S[Ee_S[ID_U||K||H(K)]]$ and gets gets $[ID_U||K||H(K)]$.

b. Calculate hash of K i.e. H'(K) and check if H'(K)==H(K), which means that request was not altered,

3. The service layer sends data to Geo-portal, (actually the service layer takes data from the database layer which will be detailed in section 3.5.2). The service layer sends encrypted spatial data to Geoportal. Spatial data may include maps, geo-referenced images etc. It sends Ee_G[SpatialData].

4. The geoportal layer gets encrypted spatial data, which is then decrypted by the geoportal layer to get the required spatial information. $Dd_G[Ee_G$[SpatialData]] and gets [SpatialData].

3.5.2 Service layer and Database layer

In addition to notations in section 3.5.1 few more notations are used here. Which are

(e_D,d_D): (public, private) key of database layer

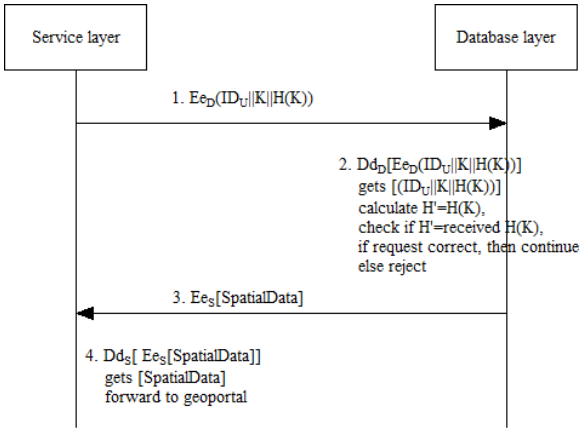

Figure 9:Secure service calls between the Service Layer and database layer

Figure 9 shows how service calls are done securely between the service layer and the database layer. Following steps are followed,

1. Request when validated in section 3.5.1 is forwarded to the database layer ($Ee_D(ID_U||K||H(K))$), this request includes K= (ServiceID||Location||Resolution), Hash of 'K' and Identity of user who requested the information.

2. Spatial Database layer, database checks of request is correct

a. Database layer decrypts request received from the service layer and gets[(IDU||K||H(K))] i.e. Identity of user, (ServiceID||Location||Resolution) and Hash of (ServiceID||Location||Resolution).

b. Calculates H'= hash of K=(ServiceID||Location||Resolution) , checks if H'= received H(K).

3. The database layer sends encrypted spatial data from the database to the service layer. Which is later sent by service layer to geo-portal layer.

4. Security Analysis of Secure SDI

The proposed secure spatial data infrastructure is implemented using ECC based public-key cryptosystem. Public key cryptographic techniques are secure and ECC based cryptosystems provide the highest level of security.Detailed security analysis is done in further sections.

Proof of Concept: Is the system secure?

Proposed secure spatial data infrastructure is implemented using elliptic curve cryptography, and is secured by following mathematical hard problems,

1. *Elliptic curve discrete logarithm problem (ECDLP)*
2. *Elliptic curve factorization problem (ECFP).*
3. *Elliptic curve computational Diffie Hellman problem (ECCDHP)*
4. *Elliptic curve decision Diffie Hellman problem (ECDDHP)*

4.1 Mathematical proof of concept by hypothesis testing

1. μ_0: Null Hypothesis =spatial data infrastructure is secure

2. μ_1:Alternative Hypothesis: There exists an attack thatthe proposed SDI is not able to defend and thus proposed SDI is not secure.

To reject alternative hypothesis μ_1, proposed secure SDI should defend popular attacks and satisfy cryptographic primitives.

4.2 Cryptographic Primitives

1. Confidentiality: In the proposed secure SDI, information is sent from one party to another by encryption using the x-coordinate of the shared secret key. Thus spatial information that is shared over the insecure channel is made unreadable and the confidentiality of spatial data is protected.

2. Integrity: Integrity is protected by using a hash function (H), the message is sent from source to destination along with the hash (H) of important components of the message. On receiving

3. The information at the destination, a hash of received message (H') is computed and this new hash is then compared with the received hash. If both hashes are equal i.e. (H==H'), then, the integrity of the message is protected.

4. Authentication: Authentication protocol is proposed in section 3.4, here Public key, private key pair is used for authentication. To make authentication more powerful an additional challenge is given to the user and the user's biometric details are used for additional security. All the communication in the authentication protocol is encrypted. Proposed secure SDI has 2 way and 4-factor authentication (Public Key, Private Key. Biometric and Challenge)

5. Non- repudiation: Nonrepudiation means the user should not be able to deny the messages sent by him. The messages are digitally signed by using a secret key to provide non-repudiation.

6. Key exchange (both public and private): in proposed secure SDI, keys are exchanged using elliptic curve Diffie Hellman key exchange. This exchange of keys is protected by the mathematical hard problem, which is impossible to solve and is protected by the elliptic curve discrete log problem, elliptic curve computation Diffie Hellman problem, elliptic curve decision Diffie Hellman problem (there does not exist a polynomial-time algorithm to solve this problem).

4.3 Attack Models

1. Exhaustive search attack: Exhaustive search is a brute force attack where Oscar (bad guy) searches for all possible keys and once Oscar gets the keys he/she can decrypt all messages in the future. But for elliptic curve cryptography key size is 160 bit and thus the intruder will have to try all possible combinations and will require 2^{160} trials. Which is not possible by using current supercomputing facilities in a feasible time. For each session a new key is established thus, the previous key becomes useless.

2. Known ciphertext attack: Oscar has full access to channel (active and passive), the message is sent from party A to party B. Oscar knows ciphertext only, the goal is to get the key and decrypt all further communication. This attack is not possible in the proposed secure SDI as there is no one to one correspondence between plaintext and ciphertext. Oscar cannot do an active attack because this will be caught as two hashes will be different and the message will be discarded at the receiver side.

3. Known Plaintext attack: Oscar knows plaintext and ciphertext (P_i,C_i), i=1,2…k. from some old communication. The goal of Oscar is to get a key. Similar to known ciphertext attack known-plaintext attack is not possible on proposed secure SDI.

4. Chosen Plaintext attack: Oscar or adversary can choose P_i and get corresponding C_i, This (P_i,C_i) pair is known to Oscar. We are giving access to the encryption machine to Oscar for some time without disclosing the key. The goal is to get a key, Oscar cannot get the key as there is a new key for each session.

5. Chosen ciphertext attack: Access of decryption machinery is given to Oscar, or the adversary can choose C_i and get the corresponding P_i. Oscar knows (C_i, P_i), i=1,2…k. A chosen ciphertext

attack is not possible on proposed secure SDI and the relationship between a public key and a private key is complex in ECC.

4.4 Attack on Elliptic curve cryptography

Security of ECC relies on the difficulty of solving the following three problems given in section 4.1

1. Solving Elliptic curve Discrete log Problem: discrete log problem is difficult to break as there is no polynomial-time algorithm to solve ECDLP. However, there are few methods in literature by which DLP can be solved but it needs huge time and memory. These algorithms include brute force, table lookup, Shanks algorithm, Pohlig-Hellman algorithm.

2. Solving Elliptic curve computation Diffie Hellman Problem: these subsequent problems are dependent on solving DLP, ECDLP. There is no polynomial-time algorithm in the literature to solve these problems.

3. Solving Elliptic curve decision Diffie Hellman Problem: this problem also relies on DLP, ECDLP, ECDHP. There is no polynomial-time algorithm to solve this problem.

4.5 Defense against Popular Attack

1. Man-in-the-middle: The intruder can act as a man in the middle between the user and geo-portal or man in the middle between the geo-portal and service layer. However, there is a strong authentication mechanism that uses 4 factors to authenticate the user to the system and system to the user. Also, there is a mutual key agreement that needs to be done before taking part in communication.

2. DoS attack: Sending multiple requests till the system crashes is a denial of service attack, here in the proposed secure SDI, one request is handled for each client. Also after three unsuccessful login attempts the user is denied access to the system. Thus, the DoS attack is not possible on proposed secure SDI.

3. Device theft attack: If a mobile device or laptop is stolen, then the thief is not able to get data from secure SDI, as he/she will have to get authenticated (4 factors) by giving biometric details and authentication will fail in this case.

4.6 Summary of security analysis of proposed secure SDI

Sr. No.	***Cryptographic primitives***	***Satisfy: Yes/ No***
1.	Confidentiality	*Yes*
2.	Integrity	*Yes*
3.	Mutual Authentication	*Yes*
4.	Non-Repudiation	*Yes*
5.	Key exchange	*Yes*

Table 1: Cryptographic primitives

Sr. No.	***Attack/ Attack Model***	***Defense Possible: Yes/ No***
1.	*Exhaustive search attack*	*Yes*
2.	*Known ciphertext attack*	*Yes*
3.	*Known Plaintext attack*	*Yes*

4.	*Chosen ciphertext attack*	*Yes*
5.	*Chosen Plaintext attack*	*Yes*

Table 2: Attacks on proposed secure SDI and defense

There does not exist an attack on the proposed secure SDI, thus we failed to reject the null hypothesis(μ_0: Null Hypothesis=spatial data infrastructure is secure), Thus, it is concluded that the proposed system is secure.

5. Findings of research on the use of cryptography in SDI.

The following is achieved by the use of cryptography in spatial data infrastructure,

1. With a secure authentication mechanism, who is accessing spatial data is traced. Login is secured by four-factor authentication.
2. Communication between layers (Geoportal layer, service layer, and a database layer) in spatial data infrastructure was secured using cryptographic techniques.
3. Encrypted files were stored in a database, thus in case of an attack on the database,the contents of the database cannot be decrypted without four-factor authentication.
4. As SDI can have information from various organizations, the privacy of location data stored in the database is protected due to the encryption of spatial information. For example, layer of the mapservices can be encrypted for location information.
5. Proposed spatial data infrastructure is able to defend all attacks and overall security of data was enhanced.

This article has focused on the topic which has been paid very less attention in the past. However, the use of cryptography in SDI cannotbe neglected.In the future, security should be considered an integral part of SDI.

6. Conclusions and Future work

With the rising demand for spatial data and the associated infrastructure for decision-making technology, the need to protect the SDI comes up. Safe SDI architecture was suggested in this article. Different SDI technologies were suggested, and a stable protocol for authentication was also suggested. Secure service call protocols also maintained cooperation between parties.Public-key cryptosystem (elliptic curve cryptography) is used in this paper to improve security. The system has also been found to be secure against common assaults to date. The system is stable until there is no polynomial-time algorithm to solve complicated mathematical issues such as "discrete logarithm elliptic curve problem"

Besides offering secure SDI, work on numerous services offered by SDI is necessary. Implementing each service by using GIS tools by conducting geographical analysis and securing each service provided by SDI needs attention. The extension of this work would be to incorporate each service, host it on a cloud server, and secure the spatial data infrastructure.

Acknowledgments: Authors are thankful to the Faculty Development Center (Geoinformatics, Spatial Computing, and Big Data Analytics) at VeermataJijabai Technological Institute, Mumbai. Also, authors are thankful to guest editors and anaonymous reviewers for their comments which has improved the quality of this manuscript.

References

[1] Rajabifard, Abbas, and Ian P. Williamson. "Spatial data infrastructures: concept, SDI hierarchy and future directions." (2001).

[2] Burrough, Peter A., and Ian Masser, eds. *European Geographic Information Infrastructures: Opportunities and Pitfalls-GISDATA 5*. CRC Press, 2003.

[3] Reed, Carl N. "The open geospatial consortium and web services standards." *Geospatial Web Services: Advances in Information Interoperability*. IGI Global, 2011. 1-16.

[4] Nogueras-Iso, Javier, et al. "OGC Catalog Services: a key element for the development of Spatial Data Infrastructures." *Computers & Geosciences* 31.2 (2005): 199-209.

[5] Acharya, P. S., and S. Pandey. "National Spatial Data Infrastructure India (NSDI-India)—Present Status and the Future Strategies." *Geospatial Infrastructure, Applications and Technologies: India Case Studies*. Springer, Singapore, 2018. 7-16.

[6] Goodchild, Michael F., Pinde Fu, and Paul Rich. "Sharing geographic information: an assessment of the Geospatial One-Stop." *Annals of the Association of American Geographers* 97.2 (2007): 250-266.

[7] Van der Wel, Frans JM. "Spatial data infrastructure for meteorological and climatic data." *Meteorological Applications* 12.1 (2005): 7-8.

[8] Bernard, Lars, and Max Craglia. "SDI-from spatial data infrastructure to service driven infrastructure." *Research Workshop on Cross-Learning Between Spatial Data Infrastructures and Information Infrastructures, Enschede, The Netherlands*. 2005.

[9] Janssen, K. A. T. L. E. E. N., and Jos Dumortier. "Legal framework for a European Union spatial data infrastructure: Uncrossing the wires." *Research and Theory in Advancing Spatial Data Infrastructure Concepts. ESRI Press, Redlands California* (2007): 231-244.

[10] Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." *IEEE transactions on Information Theory* 22.6 (1976): 644-654.

[11] Koblitz, Neal. "Elliptic curve cryptosystems." *Mathematics of computation* 48.177 (1987): 203-209.

[12] Khandare, Nikhil B., and Narendra S. Chaudhari. "Secure Sharing of Location Data Using Elliptic Curve Cryptography." *International Conference on Intelligent Computing and Smart Communication 2019*. Springer, Singapore, 2020.

[13] Maguire, David J., and Paul A. Longley. "The emergence of geoportals and their role in spatial data infrastructures." *Computers, environment and urban systems* 29.1 (2005): 3-14.

[14] Akinci, Halil, and ÇetinCömert. "Geoportals and their role in spatial data infrastructures." *Department of Geodesy and Photogrammetry Engineering, Turkey* (2007).

[15] Stefanakis, Emmanuel, and PoulicosPrastacos. "Development of an open source-based Spatial Data Infrastructure." *Applied GIS* 4.4 (2008).

[16] Ajmi, M., et al. "Setting up a spatial data infrastructure (SDI) for the ROSELT/OSS network." *Journal of Geographic Information System* 2014 (2014).

[17] Aalders, H. J. G. L., and Harold Moellering. "Spatial data infrastructure." *Proceedings of the 20th international cartographic conference. Beijing, China*. 2001.

[18] Câmara, Gilberto, et al. "Networks of innovation and the establishment of a spatial data infrastructure in Brazil." *Information Technology for Development* 12.4 (2006): 255-272.

[19] Koblitz, Neal. "Elliptic curve cryptosystems." *Mathematics of computation* 48.177 (1987): 203-209.

[20] McCurley, Kevin S. "The discrete logarithm problem." *Proc. of Symp. in Applied Math*. Vol. 42. 1990.

[21] Ahirwal, Ram Ratan, and ManojAhke. "Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network." *International Journal of Computer Science and Information Technologies* 4.2 (2013): 363-368.

[22] FG Assis, Luiz Fernando, et al. "TerraBrasilis: A Spatial Data Analytics Infrastructure for Large-Scale Thematic Mapping†." *ISPRS International Journal of Geo-Information* 8.11 (2019).

[23] CHAFIQ, Tarik, et al. "Spatial data infrastructure. Benefits and strategy." *Analelestiintifice ale Universitatii" AlexandruIoanCuza" din Iasi-seriaGeografie* 61.1 (2015): 21-30.

[24] Vancauwenberghe, Glenn, and Bastiaan van Loenen. "Exploring the emergence of open spatial data infrastructures: analysis of recent developments and trends in Europe." *User Centric E-Government*. Springer, Cham, 2018. 23-45.

[25] Guigoz, Yaniss, et al. "Spatial data infrastructures in Africa: A gap analysis." *Journal of environmental informatics* 30.1 (2017): 53-62.

[26] Chias, Pilár, and Tómas Abad. "Spatial data infrastructures and Spanish cultural heritage: The INSPIRE framework applied to the Monastery of El Escorial." *Journal of Map & Geography Libraries* 11.2 (2015): 245-265.

[27] Dawidowicz, Agnieszka, and RyszardZrobek. "Hierarchical development of the spatial data infrastructures as a globalization trend." *2016 Baltic Geodetic Congress (BGC Geomatics)*. IEEE, 2016.

[28] Arctic, S. D. I. "Arctic Spatial Data Infrastructure Framework Document." *Arctic SDI National Contact Points* (2015).

[29] Dutta, Rishiraj, and SusanthaJayasinghe. "Integrating Spatial Data Infrastructure in Monitoring Climate Change Impacts: A Research Oriented Approach." *Approach (TS-3: SDI Development* (2015).

[30] Kim, Moongie, InsunGwak, and JunehwanKoh. "The strategies of advanced local spatial data infrastructure for Seoul Metropolitan Government." *International Journal of Urban Sciences* 23.3 (2019): 352-368.

[31] Mwange, Collins, Galcano Canny Mulaku, and David N. Siriba. "Reviewing the status of national spatial data infrastructures in Africa." *Survey review* 50.360 (2018): 191-200.

[32] Murat, M. E. H. A. "Implementing a National Spatial Data Infrastructure for a Modern Kosovo." (2015).

[33] Cetl, Vlado, et al. "Establishing common ground through INSPIRE: the legally-driven European spatial data infrastructure." *Service-Oriented Mapping*. Springer, Cham, 2019. 63-84.

[34] Oliveira, Italo Lopes, et al. "Specifying the Computation viewpoints for a corporate Spatial Data Infrastructure using ICA's formal model." *International Conference on Computational Science and Its Applications*. Springer, Cham, 2016.

[35] Warekuromor, Tubolayefa, et al. "A distributed, scalable and provenance-enabled data access protocol for spatial data infrastructure." *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 2017.

[36] Kmoch, Alexander, et al. "A spatial data infrastructure approach for the characterization of new zealand's groundwater systems." *Transactions in GIS* 20.4 (2016): 626-641.

[37] Abramic, Andrej, et al. "A spatial data infrastructure for environmental noise data in Europe." *International journal of environmental research and public health* 14.7 (2017): 726.

[38] Tavra, Marina, NiksaJajac, and VladoCetl. "Marine spatial data infrastructure development framework: Croatia case study." *ISPRS International Journal of Geo-Information* 6.4 (2017): 117.

[39] Zwirowicz-Rutkowska, Agnieszka. "Evaluating spatial data infrastructure as a data source for land surveying." *Journal of Surveying Engineering* 142.4 (2016): 05016002.

[40] Zwirowicz-Rutkowska, Agnieszka. "A multi-criteria method for assessment of spatial data infrastructure effectiveness." *Earth Science Informatics* 10.3 (2017): 369-382.

[41] Coleman, David J., Abbas Rajabifard, and Kris W. Kolodziej. "Expanding the SDI environment: comparing current spatial data infrastructure with emerging indoor location-based services." *International Journal of Digital Earth* 9.6 (2016): 629-647.

[42] Bhatt, Smriti, and Ravi Sandhu. "ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things."

[43] Bhattacharjee, Shrutilipi, PabitraMitra, and Soumya K. Ghosh. "Spatial interpolation to predict missing attributes in GIS using semantic kriging." *IEEE Transactions on Geoscience and Remote Sensing* 52.8 (2013): 4771-4780.

[44] Ramachandra, T. V., A. H. Bharath, and M. V. Sowmyashree. "Monitoring urbanization and its implications in a mega city from space: Spatiotemporal patterns and its indicators." *Journal of environmental management* 148 (2015): 67-81.

[45] Shekhar, Shashi, Chang-Tien Lu, and Pusheng Zhang. "Detecting graph-based spatial outliers: algorithms and applications (a summary of results)." *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining*. 2001.

[46] Gupta, Ajay, and Nandlal L. Sarda. "Efficient evacuation planning for large cities." *International Conference on Database and Expert Systems Applications*. Springer, Cham, 2014.

[47] Grothe, M., et al. "Smart Emission-Building a Spatial Data Infrastructure for an Environmental Citizen Sensor Network." (2016).

[48] Innerebner, Markus, et al. "Organizing earth observation data inside a spatial data infrastructure." *Earth Science Informatics* 10.1 (2017): 55-68.

[49] Idrees, Mohammed OludareIdrees. "Challenges in coastal spatial data infrastructure implementation: A review." *South African Journal of Geomatics* 4.4 (2015): 369-383.

[50] Idrees, Mohammed OludareIdrees. "Challenges in coastal spatial data infrastructure implementation: A review." *South African Journal of Geomatics* 4.4 (2015): 369-383.

[51] Bui, Quang Hung, et al. "Spatial Data Infrastructure." *TORUS 2–Toward an Open Resource Using Services: Cloud Computing for Environmental Data* (2020): 247-261.

[52] Iban, Muzaffer Can, and OktayAksu. "A model for big spatial rural data infrastructure in Turkey: Sensor-driven and integrative approach." *Land Use Policy* 91 (2020): 104376.

[53] Kiwelekar, Arvind W., et al. "Deep Learning Techniques for Geospatial Data Analysis." Machine Learning Paradigms. Springer, Cham, 2020. 63-81.