International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 4, Jul-Aug 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

The Role of Cybersecurity in Remote Sensing and Geographical Information System (GIS)

Felix Ale[1], Abdullahi Ayegba[2], Emmanuel Omomoh[3], Gujahar Rengje Danlami Rogers[4], Urukwe Ando[5], Desmond Wysenyuy[6], Oyibo Muazu[7], Iruemi Olohimai Juliet[8], Ndahi Aisha[9]

[1,2,8]Engineering and Space Systems Department, National Space Research and Development Agency, Abuja, Nigeria
[3]Zonal Advanced Space Technology Application Laboratory, Jos, Plateau State, Nigeria
[4]Department of Geology and Water Resources, Zonal Advanced Space Technology Application Laboratory, Jos, Plateau State, Nigeria
[5]Takum, Taraba State, Nigeria
[6]Management and Research Analysis, School of Space and Earth Observation, Arizona State University, USA
[7]Division of Astronomy, Centre for Basic Space Science, Nsukka, Enugu State, Nigeria
[9]Interplanetary Initiative, Arizona State University, USA

ABSTRACT

As a result of the importance of remote sensing and GIS data in various sectors of the country today, and taking into cognizance the sensitive nature of some of these data as well as the rising cases of cyber threats in the recent times, the role of cybersecurity in Remote sensing and GIS cannot be overemphasized. The aim of this research work was to study the role of Cybersecurity in Remote Sensing and GIS. The research made use of secondary data which includes but not limited to published research works, videos and library materials, while it adopted explanatory and descriptive research methods. The results showed that cybersecurity when integrated with Remote Sensing and GIS will help in the protection of the satellite or spatial images against cyberattacks, ensures the data reliability and availability, as well as maintain data integrity and confidentiality. In addition, it was observed from the results that cybersecurity can be integrated with GIS and Remote sensing in order to achieve the above goals through data encryption, implementation of user authentication and authorization protocols, Incident Response Planning application, access control method, and others. From the results, it was concluded that Cybersecurity plays an important role in Remote sensing and GIS. It was recommended that the scope of the research should be increased to the general Space Science and Technology instead of a branch of it which is Remote Sensing and GIS studied in this work. In addition, it was also recommended that the role of Remote sensing and GIS in cybersecurity should also be carried out in future work.

KEYWORDS: *Cybersecurity, Data integrity, Data Encryption, GIS, Remote Sensing*

How to cite this paper: Felix Ale | Abdullahi Ayegba | Emmanuel Omomoh | Gujahar Rengje Danlami Rogers | Urukwe Ando | Desmond Wysenyuy | Oyibo Muazu | Iruemi Olohimai Juliet | Ndahi Aisha "The Role of Cybersecurity in Remote Sensing and Geographical Information System (GIS)" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-4, August 2024, pp.308-312, URL: www.ijtsrd.com/papers/ijtsrd67150.pdf

IJTSRD67150

Copyright © 2024 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

Remote sensing is defined as the process of acquiring signal from an object or area without having physical contact with that object or area, while Geographical Information System (GIS) is defined as a computerized tool for the acquisition, storage, checking, retrieval, integration, manipulation, analysis and display of data, which are spatially referenced to the earth., (Burrough, 1989).

The term, Cyber security, is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement (Seema et al., 2018 and Ayegba *et al.*,

2024). Cyber systems form the central infrastructure of critical sectors as nearly all of them utilize Information Technology to facilitate core business processes (Silvance, 2019). So far, technological innovation has created opportunities for companies to carry out online transactions through the internet, which are constantly growing worldwide. But this internet has become a key medium for cybercriminals to perfume several cybercrime-related activities. According to studies, lack of understanding of cybersecurity attacks and threats is one of the driving factors leading to the growing number of internet-related attacks (Adamu, 2022). The exponential growth in modern technologies has changed many lives, particularly the communication channels used to widely disseminate information and to interact with others in real time. Various communication techniques have been developed worldwide, thus, making public and private sectors to offer more services and adopt new technologies to provide access to information anytime and anywhere upon request from customers. In response, the number of hackers and organized cybercrime groups has grown exponentially (Talal and Asifa, 2021).

Unfortunately, Hackers can also earn money by selling secret data to competitors on the dark web, which makes cyberspace unsafe and poses considerable risks to organizations and their customers. As a result of this situation, cybersecurity breaches have become a serious threat to global security and the economy, targeting critical infrastructure and having a considerable financial impact on business performance and results in a significant loss of intellectual property (Garg, 2003).

2. Methodology

The research method used in the work is qualitative research method. The qualitative research types used were descriptive and explanatory research methos. The methods were used to enable the authors explain and analyse various points relating to the topic of studies. In addition, secondary data ranging from library materials, internet sources, published books, video are the materials used for the work.

3. Results and Discussion

This section answers the research question which is "what are the roles of Cybersecurity in Remote sensing and GIS?"

3.1. Some roles of cybersecurity in remote sensing and GIS are as follows:

A. Data Encryption application: Spatial data or satellite imagery are very important in security, health, education as well as other aspects of the economy or in our everyday lives. These data are sometimes processed data, pre-processed data or even raw data, and are sent or transferred from one place to another for processing and analysis for its application. This data is supposed to be in its original form as any alteration will change the message or the interpretation that it should carry. For instance, the satellite imagery that is to be used for change detection analysis, when not properly secured, or when a wrong one is given out to users, it will not give the correct result when processed. Some satellite imageries are used for security purposes, and the change detection can be part of it. This is because, it will help in checking if there are new human or strange activities in some suspected places. There is need to adopt proper security measures to prevent the tampering with of the satellite imagery or data before it reaches the intended users. This can be achieved through cybersecurity idea or methods such as converting the image or data into codes. By so doing, it is only the authorized person with the code that can access or open the document to know what it contains. For instance, when some banks are sending statement of accounts at the end of the months to the customers, a message will be attached that the document can be opened using account number or password only or Pension ID in the case of pensions. With this encryption, it will be impossible for unauthorized person to access the document or information. This code used to open the document is called the decryption code or key. Satellite images or data need this encryption too.

B. Protecting sensitive Remote Sensing and GIS data or information: Protection of Remote Sensing and GIS data involves the various measures to safeguarding or shielding RS and GIS data from distortion, harm, danger, or loss. It involves the various measures taken to prevent potential threats, risks, or vulnerabilities of data, and also ensuring the security as well as safety and reliability of the data. Remote sensing and GIS systems handle sensitive information, which must be protected from unauthorized access or manipulation. Apart from satellite imagery or data, spatial or field data are also sensitive information, any alteration of any aspect may make the entire message or interpretation different from the original one. For instance, if a rocket is to be lunched from point A to B, and the coordinates are to be used to calculate the distance or range between the two points, allowing free access to such an information could lead to the manipulation of the data, and the results will not be as expected. It is also applicable in satellite data application and

analysis. When a wrong imagery is substituted for the main or needed one, the entire result is already bad from that point. That is why proper protection is needed in remote sensing and GIS, hence the role of cybersecurity.

C. **Cybersecurity secures Data Storage application:** Data storage security is defined as the protection of storage resources and the data stored on from accidental or intentional damage, and from unauthorized users and uses. Secure Data Storage deals with the computing processes and technologies used to ensure stored data security and integrity. This can include physical protection of the hardware on which the data is stored, as well as security software. This can be achieved through various measures like regulating the accessibility to each data storage device/software, protection of data storage devices and data itself against viruses, worms and other data corruption threats, storage device and infrastructure security, adoption as well as implementation of layered storage security architecture.

D. **It helps in Incident Response Plan:** Incident response planning is defined as a structured process to detecting, responding to, and managing cybersecurity incidents, such as data breaches, ransomware attacks, or denial-of-service attacks. It is also defined as the instructions on how to respond to a serious security incident, such as a data breach, data leak, ransomware attack, or loss of sensitive information. The Cybersecurity Incident Response Plan helps to quickly mitigate the impact, contain the damage, and restore normal operations. This is achieved through the identification potential risks, establish a response team, and define communication channels; Monitor for suspicious activity and detect potential incidents; Isolate affected systems and Restore systems and data, and confirm normal operations.

E. **It helps Data Access Control:** Data Access Control is a method that allows organizations to authorize users, employees and/or third parties to access the data of an organisation in a manner that meets security, privacy and compliance requirements. These security, privacy and compliance requirements are set by security best practices and official regulations. These regulations often require organizations to audit and place controls over the entities that can access sensitive information. Access control determines what one party will allow another party to do with respect to the data or information regulated or coordinated by the former. Access control usually requires authentication as a prerequisite (Ravi and Pierangela, 1994). When spatial data in a database is accessible to everyone, the integrity of the data will be questionable. The data can be given out at any time by anyone including the classified or restricted ones. In addition, as a result of the free accessibility of everyone in the organization to the data or information, even wrong data can be given out to intending users and they may not know that it was a wrong or manipulated satellite or spatial data. A satellite imagery needed for land use land cover analysis or the image needed for erosion mapping of a particular place needs to be an updated or recent one. This data will be more reliable if it is gotten from a particular source in an organization in charge of the Archiving and who is solely authorised to do so. He or she would not give out a wrong data since he or she knows that the wrong data when noticed would affect the organization or unit. He or she will tell the users the truth when the needed satellite or spatial data is not available instead of providing them with a manipulated data. Controlling access to sensitive data and systems, and ensuring that only authorized personnel can access and modify information is very important in remote sensing and GIS data analysis or system.

F. **Intrusion Detection application:** An Intrusion Detection System is a security tool that monitors a computer network or systems for malicious activities or policy violations. This is done by detecting unauthorized access, potential threats, and abnormal activities by analyzing traffic and alerting administrators to take action. It is very crucial for maintaining network security and protecting sensitive remote sensing and GIS data from cyberattacks. Cybersecurity ensures that the systems automatically detects and blocks the network attacks and browser attacks, protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways (Ishu *et al., 2022*). Data intrusion detection in remote sensing and GIS can be achieved through some means such as monitoring of Satellite Data Transmissions, identify unusual patterns or behavior in the data transmissions, check for known attack patterns or malware signatures in the data and analysing the behavior of the data transmissions to detect potential threats, etc.

G. **Secure Cloud Computing:** Most businesses have shifted to the cloud for these services due to its

several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others. Cloud computing is a paradigm that enables huge memory space and massive computation capacity at a low cost. It allows users to obtain the intended services across multiple platforms irrespective of location and time (ISHU et al, 2022). Cloud security is an aspect of cybersecurity dedicated to securing cloud computing systems. It deals with keeping data private and safe across online-based infrastructure, applications, and platforms. Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection. Cloud security will help to protect a remote sensing and GIS data from attacks, malware, hackers, and unauthorized user access or use. Using secure cloud services for data storage, processing, and collaboration will ensure GIS data privacy and security.

H. Authentication and Authorization: Authentication helps to establish the identity of one party to another. Most commonly authentication establishes the identity of a user to some part of the system typically by means of a password. Also, authentication can be computer-to-computer or process-to-process and mutual in both directions (Ravi and Pierangela, 1994). Controlling access to GIS systems and data through secure login credentials (authentication) and limiting access to specific resources based on user roles and permissions (authorization) is very important. Also, Multi-Factor Authentication offer an additional layer of access security to sensitive systems and applications while application white-listing prevents staff from installing unapproved and potentially malicious programs (Silvance, 2019). This mechanism will make the server or archives safe and free from attacks.

3.2. Why is cybersecurity important in Remote Sensing and GIS

A. To maintain data integrity: The integration of Cybersecurity into remote sensing and GIS will bring about data integrity. Data integrity is defined as the maintenance of data accuracy and consistency. Data integrity is the process of protecting information from being modified by unauthorized parties. The basic principles of data integrity are Attributable, Legible, Contemporaneous, Original, and Accurate. Standard measures to guarantee integrity are Cryptographic checksums, Using file permissions, Uninterrupted power supplies, Data backups (Gupta *et al.,* 2018). Cybersecurity ensures the accuracy and reliability of remote sensing data and GIS analysis, preventing data tampering or manipulation. It will ensure that the integrity of remote sensing and spatial data is maintained through various measures.

B. Preventing cyberattacks: A cyberattack is defined as any intentional effort to alter, steal, expose, disable, or destroy data, applications, through unauthorized access to a network, computer system or digital device. Cyberattack can cause total loss of spatial data or have it corrupted. But with proper protection measures using cybersecurity, the data will be safe and secured. Integrating cybersecurity measures prevents attacks on remote sensing and GIS systems, reducing the risk of system compromise or data breaches.

C. Ensuring confidentiality: This deals with restricting data access strictly to authorised personnel. Systems users have a responsibility to ensure they maintain secure access control systems, including both logical and physical restrictions such. By this, it is very important that all employees of an organisation receive thorough training in information or cyber security awareness and best practices in order to be up-to - date. Cybersecurity ensures that remote sensing data and GIS information are only accessible to authorized personnel, thus maintaining its confidentiality.

D. Data Availability: Data availability means guaranteeing reliable access to information or data by authorised personnel. Data must be stored in a secure system in order to be readily accessible always. High availability of Remote sensing and GIS data will be beneficial to the country, individuals or groups especially researchers and policymakers. When data of GIS is well secured, it will be available for many years come.

E. Cybersecurity enables data reliability: Reliability is defined as the dependability and consistency of a system, process or thing. It is the ability of a system or something perform its function or role without error or failure. Data reliability defined as the dependability and consistency of a data, and in this case, a remote sensing and GIS data. Data reliability guarantees data integrity initiatives data security, and data

quality. Cybersecurity ensures accurate and reliable remote sensing data and GIS analysis for decision-making in various fields or sectors of the country.

F. It promotes national security: Integrating cybersecurity with remote sensing and GIS supports national security by protecting sensitive information and preventing cyberthreats and attacks. This is because, application of remote sensing and GIS can be found in agriculture, security, health, water, transportation, energy, planning, environment, telecommunication, and so on. The securing of the information or data from any of these especially the sensitive ones will enhance national security, and supports national growth and development.

4. Conclusion

This research work looks at the roles of Cybersecurity in Remote Sensing and GIS considering the importance of and various applications of remote sensing and GIS in various aspects of the country. The research made use of qualitative research method to discuss and analyse the secondary data obtained from the library, published works, online and other sources. The results showed that cybersecurity application in Remote Sensing and GIS will help in protecting the satellite or spatial images against cyberattacks, ensures the data reliability and availability, as well as maintain data integrity and confidentiality. In addition, it was observed from the results that cybersecurity can be applied in or integrated with GIS and Remote sensing in order to achieve the above goals through data encryption, implementation of user authentication and authorization protocols, Incident Response Planning application, access control method, secure cloud computing and others. From the results, it can be concluded that Cybersecurity plays an important role in Remote sensing and GIS which will ensure a reliable, secured and unauthorisedly accessed spatial data that can be used for national security, planning, economic development and overall national growth.

5. Recommendation

We recommend that the scope of the future research in this area be expanded to the application of Cybersecurity in Space Science and Technology in general instead of a branch of it which is Remote Sensing and GIS studied in this work. Also, it is also recommended that the role of Remote sensing and GIS in cybersecurity should be carried out in future work.

References

[1] Abdullahi Ayegba, Hayatu Idris Bulama, Oyekunle Oluwatoyin Victoria, Idris Shehu, Adejoh Joshua, Omakoji Odiba, Oyibo David (2024): "An Assessment of Some Dangers Associated with the Use of Pirated Software on Computers" Published in International Journal of Trend in Scientific Research and Development, Vol. 8(3), pp.981-985.

[2] Adamu Abdullahi Garba, Maheyzah Muhamad Siraj, Siti Hajar Othman (2022): An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering (IJECE) Vol. 12, No. 1, February 2022, pp. 572~584

[3] B. B. Gupta, D. P. Agrawal, Haoxiang Wang (2018): Computer and CyberSecurity: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335,

[4] Burrough Peter (1989): Principles of Geographic Information Systems; Oxford Science Publications: New York, USA.

[5] Garg, A.; Curtis, J.; Halper, H. (2003): Quantifying the financial impact of IT security breaches. Inf. Manag. Comput. Secur. pp 11, 74–83.

[6] Seema P. S, Nandhi Sundaresan, Sowmiya M (2018): Overview of Cyber Security. DOI: 10.17148/ijarcce.2018.71127

[7] Silvance Abeka (2019): Cyber Physical System Security Model For Remote Sensing Device Protection: A Technical Review. International Journal of Computer Trends and Technology. Volume 67 Issue 9. Pp 65 – 77.

[8] Ravi Sandhu and Pierangela Samariti (1994): Access Control: Principles and Practice. www.cerias.purdue.edu>.

[9] Talal Alharb and Asifa Tassaddiq (2021): Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data Cogn. Comput. 2021, 5, 23. https://doi.org/ 10.3390/bdcc5020023