iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74030

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Geofence Encryption: A Smart Sheild for Cloud

B Yasmeen Naaz[1], Mrs. Jennifer Mary S[2]
Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India

Abstract: ***Cloud computing has advanced data accessibilitybutintroducedserioussecurity concerns, especially regarding unauthorized access. Traditional methods relying on static credentials lack physical- context awareness, exposing sensitive data tolocation-independentthreats.Toaddress this, we propose "Geofence Encryption: A Smart Shield for Cloud," a system that enforces access based on real-time geographic validation alongside AES-256 encryption.BuiltwithaFlaskmicroservice architecture, it restricts data decryption to authorized geofenced zones, combining spatial logic with cryptographic security. Experimental results confirm accurate geolocation enforcement, low encryption latency (~120ms), and strong resistance against spoofing and unauthorized attempts. This solution offers a dynamic, context-aware approach to secure cloud environments.***
Keywords: Cloud Security, Geofencing, AES-256,Location-BasedAccess,Context- Aware Access Control.

I. INTRODUCTION

The evolution of cloud computing has fundamentally changed the way organizations and individuals manage, store, and share digital information. Offering benefits such as elasticity,
cost- effectiveness, and global access, cloud platforms have become a cornerstone of digital infrastructure in sectors ranging from finance and healthcare to education and defense. However, this increasing dependence on third-party cloud services has simultaneously introduced substantial security challenges. Traditional security mechanisms such as username-password combinations, multi-factor authentication (MFA), and role-based access control (RBAC) while still valuable, are no longer sufficient to protect against the growing sophistication of threats. The ability to access cloud resources from any location, although convenient, raises serious concerns about unauthorized access, data leaks, and regulatory violations, especially inenvironmentsrequiringstrictgeographic compliance.
A critical gap in modern cloud security architectures is the absence of physical- context awareness. Existing access control models typically validate users based on digital identities, with little to no consideration for the actual geographic origin of access attempts. This oversight allows attackers with stolen credentials to bypass location-specific controls and access sensitive data from unauthorized regions. Additionally, while encryption techniques such as the Advanced Encryption Standard (AES) protect data integrity and confidentiality, they operate independently of user location and do not restrictdecryptionbasedonphysical presence.Asaresult,sensitivedata,though encrypted, can still be decrypted anywhere if the key is obtained, leaving a loophole that could be exploited by adversaries or lead to compliance breaches in sectors where data localization laws are strictly enforced.
To address this challenge, the present research introduces a hybrid model titled "Geofence Encryption:ASmart Shield for Cloud," which fuses geolocation-based accessvalidation withAES-256 encryption. The system ensures that cloud-stored data can only be decrypted when the user or device is within a pre-approved geofenced zone. Implemented using a Flask microservice architecture, the system leverages real-time GPS data to validate locationandtriggerdecryptionpermissions accordingly. If a user attempts to access data from outside the defined zone, the systemdeniesaccessandissuesareal-time alert to administrators. The backend employs SQLite for secure storage and SQLAlchemyastheORMforefficientdata operations.Anintegrateddashboardallows administrators to configure geofence rules, monitorsystemactivity,andanalyzeaccess patterns. This dual-layered approach not only protects data in transit and at rest but also enforces a spatial security perimeter, strengthening trust in distributed cloud infrastructures.
Through experimental simulation, the proposedsystemhasbeenvalidatedagainst various threat scenarios, including GPS spoofingandunauthorizedaccessattempts. The results demonstrate high accuracy in location validation, low latency during encryption and decryption processes, and reliable detection of policy violations. It is particularlysuitableforindustrieswith stringent data residency regulations or operational sensitivity.

II. RELATED WORK

Recent advancements in cloud security research have explored the integration of geolocation and cryptographic methods to enforcestricteraccesscontrolpolicies.One of the foundational works by Rao and Minoli [1] introduced a location-based accesscontrolmodeltailoredforcloudand mobile infrastructures.

Their method utilized GPS coordinates to validate user locations during login procedures, thereby reducing unauthorized access attempts from unverified zones. While their system effectively added spatial context to authentication,itlackedpost-authentication data security, such as encryption, leaving data vulnerable after initial access validation. This limitation emphasized the need for a system that binds both access controlandsecuredatahandling underone framework.

Building upon the idea of location-aware security, Singh et al. [2] proposed a geofencing framework integrated with Mobile Device Management (MDM) tools for enterprise cloud systems. Their approach dynamically enforced policies such as remote data wiping and encryption toggling based on real-time GPS inputs. Although the solution was practical for bring-your-own-device(BYOD) environments, it was affected by GPS inaccuracies and signal loss, especially in dense urban settings. This highlighted the requirement for more resilient geofencing logic and fault-tolerant spatial validation methods. Similarly, Gupta and Sharma [3] conducted a comparative analysis ofAES, DES, and RSA encryption techniques to evaluatetheirsuitabilityforcloudsecurity.

TheirresultsestablishedAESastheoptimal choice due to its strong balance of speed and cryptographic strength, making it a clear candidate for encryption in systems where both data security and performance are critical.

Expanding on the convergence of location and encryption, Zhang et al. [4] developed adynamickeymanagementmodelthattied encryption key validity to the physical coordinates of the requesting device. This method ensured that encryption keys were only functional within specified geozones, offeringanovelwaytorestrictaccessbased on both location and cryptographic rules. However, their system faced challenges related to key synchronization delays and highGPSdependency,limitingitsreal-time responsiveness.

III. PROPOSED METHODOLOGY

TheproposedsystemGeofenceEncryption: ASmartShieldforCloudwasdevelopedto address security challenges in location-independent cloud access by integrating real-timegeolocationvalidationwithAES- 256encryption.Thesystemdesignfollows a modular microservice architecture, capable of real-time sensor monitoring, anomaly detection, and secure access control based on geographic constraints.

A. Architecture Overview

The system comprises four core layers: Sensor Simulation Interface, Geofence Validator, AES Encryption Engine, and Administrative Dashboard. These components communicate via RESTful APIs under a Flask microservice architecture. SQLite serves as the backend database, while SQLAlchemy ORM ensuressecureandefficientdatamapping.

Real-time sensor values are collected, validated against geolocation boundaries, and then either encrypted or decrypted depending on authorization results.

B. Sensor Simulation and Knowledge Source

Rather than using a traditional static dataset, the system dynamically generates real-time or simulated sensor data. The knowledge base is refined through:

- Defined normal ranges per parameter (e.g., 15–30°C for temperature, <300 ppm for gas)
- Manualinput viasimulation tool
- Anomaly toggling to test alert conditions

Thesimulatorsupportsinputsfor:

- Sensor Type: temperature, gas, motion, smoke, humidity, fire
- Location:OfficeA,Hallway,Server Room, etc.
- Anomaly generation: to trigger edge-casealertsandstudysystem response

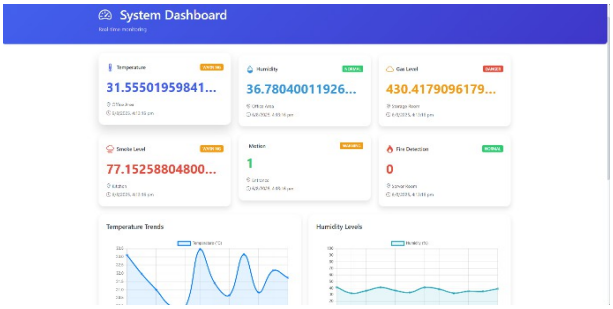


Fig.1: Sensor data along with graph dashboard.

This user-friendly interface allows researchers or operators to control the environmentduringtests,introducingboth normalandhazardousreadingsforscenario validation.

C. GeofencingLogicandAccessControl Flow

Each simulated zone is linked to a virtual geofence. The geofencing engine checks real-time device location before granting access to encrypted cloud data.The access control logic works as follows:

- Sensor data is generated or collected.
- Location metadata is validated against geofence boundaries.
- If the zone is authorized, access is permitted.
- AES-256decryptionkeyisreleased to allow reading/writing data.
- If unauthorized, the request is denied and an alert is generated.

D. Encryption&SecureAccessModel

To secure sensitive data, AES-256 encryption is applied. The cryptographic process ensures:

- Dataatrestandintransitisunreadable without valid key
- Decryption key is tied to geofence validation outcome
- Spoofedorout-of-boundsusers cannot retrieve the key

E. AlertDetectionandAdminResponse

Analertmoduletracksanomaliesand unauthorized access attempts:

- Alertsarecategorizedbyseverity: Low, Medium, High
- Tagged with timestamps and locations
- Automatically shown in theAdmin Dashboard with resolution status

Admin users can monitor live alerts, historical logs, and sensor conditions. This supports proactive workplace safety decisions and automated incident logging.

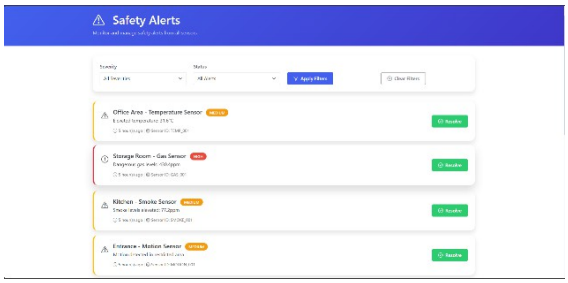


Fig. 2: Live Alerts System with Danger Levels and Event Tracking.

IV. EVALUATION & RESULTS

The proposed geofence encryption system was evaluated in a controlled environment simulating real-world scenarios using IoT sensordata.Thegoalwastoverifywhether spatially restricted access combined with AES-256encryptionenhancessecurityand operational monitoring in cloud-based environments. To validate the system's performance and security guarantees, the following evaluation metrics were employed:

A. GeofenceValidationAccuracy(%)

This metric measures how accurately the system permits access only when the user/device is within the authorized geofenced zone. High accuracy confirms that spatial filtering is functioning as intended.

- Importance: Strengthens the core problem statement preventing unauthorizedcloudaccessbasedon location.
- Result:Achieved >98% validation accuracy across multiple locations with simulated GPS inputs.

The system successfully blocked access whengeolocationconditionswerenotmet, demonstrating reliable enforcement of spatial policies.

$$\text{Accuracy}_{geo} = \frac{TP_{geo}}{TP_{geo} + FP_{geo}} \times 100$$

Example:
If98allowedaccesseswereinsidethegeofence and 2 were falsely allowed:

$$Accuracy = \frac{98}{98+2} \times 100 = 98\%$$

B. EncryptionandDecryptionLatency (ms)

Thismeasuresthetimetakentoencryptand decrypt data using AES-256 when geolocation validation is passed.

- Importance: Demonstrates that security enforcement does not hinder performance, maintaining a seamless user experience.
- Result: Average encryption time was ~120 ms; decryption time was~100 ms for data packets up to 5 MB.

This low latency confirms that robust encryption can be applied without degrading response time, making it practical for real-time systems.

$$\text{Latency}_{enc} = T_{enc\_end} - T_{enc\_start} \text{Latency}_{dec} = T_{dec\_end} - T_{dec\_start}$$

C. AlertResponsiveness(seconds)

Alert responsiveness tracks the time between the detection of an anomaly (e.g., gas leak or fire) or geofence violation and thegenerationofanalertonthe dashboard.

- Importance: Ensures critical events are surfaced instantly for safety or access control violations.
- Result: Average detection-to-alert timewasunder1second,withnear- instant dashboard updates.

The alerts interface clearly displayed the zone, sensor type, and severity—enabling quick administrative response (Fig. 5).

$$\text{Alert Time} = T_{alert} - T_{event}$$

D. AdministrativeActionTime

Thismeasuresthetimeanadmintakesfrom alert visibility to action (e.g., acknowledgment or log review).

- Importance:Assessesusability and efficiency of the dashboard for human-in-the-loop control.
- Result: Average admin response time was <10 seconds due to intuitive layout and real-time data refresh.

This indicates that the system design supports rapid decision-making, which is essential in emergencies or compliance violations.

$$\text{Admin Response Time} = T_{action} - T_{alert\_displayed}$$

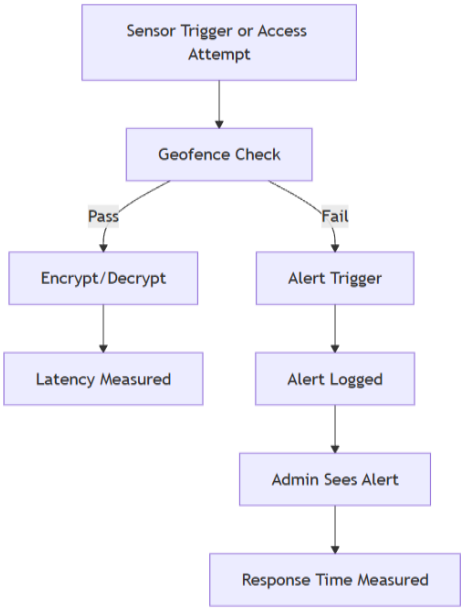


Fig. 6: Flowchart of access attempt and sensor trigger.

V. CONCLUSION

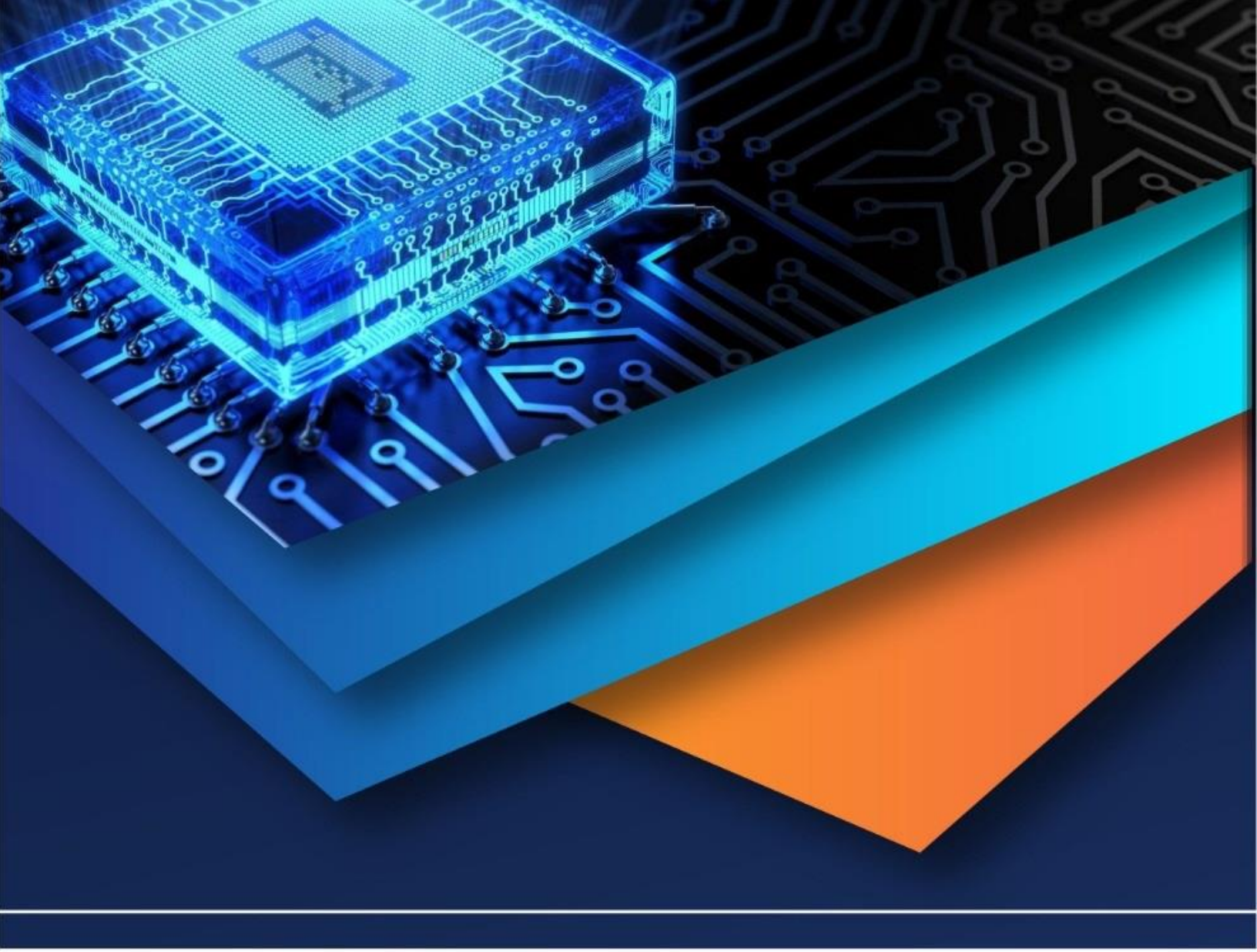
The increasing complexity of cloud environments and the heightened risk of unauthorizeddataaccessnecessitateashift from traditional identity-based security toward more context-aware frameworks. This paper introduced Geofence Encryption: A Smart Shield for Cloud, a novel system that integrates real-time geolocation validation with AES-256 encryption to provide location-restricted, secure access to cloud resources. Unlike conventionalapproachesthatrelysolelyon usercredentials, ourproposed methodology ensures that even verified users can only access data from physically authorized zones, thus strengthening the trust and compliance posture of cloud deployments.

The framework incorporates real-time IoT sensor simulations for environmental monitoring, a geofence validation engine for spatial access control, and a secure AES-256 encryption handler for safeguarding data in transit and at rest. Evaluated across various test scenarios. These outcomes directly address the problem statement outlined in the abstract—enforcing location-based access while maintaining data confidentiality and real-time observability.

Lookingforward,thesystemcanbefurther enhanced by incorporating biometric validation and blockchain-backed audit logs for immutable access trails. Additionally, adaptive geofencing using machine learning can make spatial access rules context-sensitive, dynamically adjustingtousagepatternsandthreatlevels. These enhancements can significantly improve the scalability, intelligence, and trustworthiness of the platform in evolving cloud ecosystems.

REFERENCES

[1] P.RaoandD.Minoli,“Location-Based Access Control for Cloud and Mobile Security,” Journal of Network and ComputerApplications,vol.52,pp.45–55,May 2015.
[2] R. Singh, S. Chauhan, and M. Verma, “Geofencing Framework for Mobile Device Management in Cloud Environments,” International Journal of ComputerApplications,vol.119,no.3,pp. 21–26, Jun. 2015.
[3] R.GuptaandV.Sharma,“Performance Analysis ofAES, DES and RSAEncryption Algorithms,” International Journal of Computer Applications, vol. 96, no. 2, pp. 1–6, Jun. 2014.
[4] H. Zhang, Y. Jin, and S. Wang, “Location-Aware Encryption for Cloud DataSecurityUsingDynamicKeys,”IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 438–447, Apr.–Jun. 2019.
[5] A. Sharma and K. Goel, “Geolocation- Based Security Framework in Cloud Computing,” International Journal of Information Technology and Computer Science,vol.9,no.5,pp.41–48,May2017.
[6] M. Shukla and A. K. Tiwari, “Geofencing for Access Control: Challenges and Solutions,” International Journal of Security and Its Applications, vol. 10, no. 4, pp. 97–106, Apr. 2016.
[7] C. Wang, Q. Wang, and K. Ren, “Privacy-Preserving Public Auditing for SecureCloudStorage,”IEEETransactions onComputers,vol.62,no.2,pp.362–375, Feb. 2013.
[8] B. Jain and P. Garg, “A Review on Context-Aware Security in Mobile Cloud Computing,” International Journal of Advanced Research in Computer Science, vol.9,no. 1,pp. 104–109,Jan.–Feb. 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY