iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.54993

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 11 Issue VIII Aug 2023- Available at www.ijraset.com

Data Leak Localization and Prevention using LDN

Munikrishnan[1], Sreerambabu[2], Mohammed Riyaz[3], Kalidasan[4]
[1]PG Scholar, [2]Head of The Department, [3,4]Assistant Professor Dept of MCA.

Abstract: ***While geofencing and geolocation tracking offers valuable tools for data sharing and access, it is crucial to acknowledge their potential risks and concerns. Some individuals may feel uneasy about the constant tracking and monitoring of their location, which can give rise to privacy issues. Moreover, geofencing and geolocation tracking are susceptible to hacking and cyber attacks, potentially leading to the theft or compromise of sensitive data. To address these concerns, businesses, and organizations must implement robust security measures and protocols when employing geofencing and geolocation tracking. These measures may involve encrypting sensitive data, monitoring and auditing access logs to identify potential threats or unauthorized access, and implementing user authentication and access controls to restrict data and information access. In conclusion, while geofencing and geolocation tracking can be powerful tools for data sharing and access, they should be utilized cautiously and accompanied by strong security measures to mitigate potential risks and threats.***
Index Terms: Geo-location, Data Prevention, Geofence, location-based Service, geospatial.

I. INTRODUCTION

The rise of remote work and mobile access to resources has greatly facilitated the accessibility of data from any location and at any time. However, the risks associated with accessing data from untrusted networks remain a concern for businesses, potentially leading to data loss and the exposure of critical information. To mitigate these risks, we propose implementing an innovative Virtual Fence that leverages location data and geospatial intelligence. Geospatial analysis enhances understanding, supports informed decision-making, and enables accurate predictions. A Geo-fence is a feature that establishes a virtual boundary around a real-world geographic area. When a user enters or exits this boundary, actions are triggered on their location-enabled device. Typically, the user receives real-time notifications with relevant information based on their location. The primary advantage of this technology is its seamless integration of the virtual and physical realms. Geofencing is a location-based service that utilizes GPS, RFID, Wi-Fi, or cellular data to activate predefined actions when a mobile device or RFID tag enters or exits a virtual boundary surrounding a specific geographical [8]. location called a geofence. Depending on the configuration, a geofence can trigger mobile push notifications, text messages, alerts, targeted advertisements on social media, enable vehicle fleet tracking, disable specific technologies, or provide location-based marketing data [7]. Some geofences are established to monitor activities within secure areas, allowing management to receive alerts whenever someone enters or leaves a designated zone. Businesses can also leverage geofencing to monitor employees in the field, automate timecard processes, and track company assets. Respecting privacy has always been an integral part of human existence, and its importance has only grown in today's digital age. The increasing digitization and sharing of data have heightened the significance of data privacy. Properly managing information based on its perceived importance is essential for safeguarding data privacy. Data privacy is relevant not only to businesses but also to individuals who have a vested interest in protecting their personal data. By enhancing awareness of data privacy, individuals can better shield themselves from a range of risks. This includes safeguarding financial data, medical records, social security numbers, and sensitive personal details such as birthdates, full names, and addresses. The delivery of various services through the Internet is known as cloud computing [10]. Data storage, servers, databases, networking, and software are examples of these resources, as illustrated in Both public and private clouds are possible. For a price, public cloud services deliver services via the Internet [1]. Private cloud services, on the other hand, cater to a limited number of customers. These services are a network system that provides hosted services. A hybrid option is also available, which includes components of both public and private services [9]. Cloud computing is the use of computer technology (computing) in conjunction with Internet-based development (cloud). Google Apps, for example, offers common business apps online that can be accessed through a web browser and save software and data on the server [2].

II. METHODOLOGY

The objective of this project is to provide an overview of Geo Server's authentication and authorization subsystems, covering basic/digest authentication, CAS support, and integration with various identity providers. It will showcase practical examples of custom authentication plugins for seamless integration into existing security architectures.

Additionally, the project proposes the implementation of a Geo-fencing feature that utilizes different algorithms like Ray-casting, Winding Number, TWC (Triangle Weight Characterization), and Circular Geofencing with the Haversine Formula to determine a person's presence within a specified geofence range. This geofencing system enhances security by generating alerts upon entry or exit from designated areas, and it includes a data wipeout capability. function as either active or passive barriers, based on user preferences and device settings. The objective of this research is to develop a flexible system for accurately recognizing fine expressions, capable ofhandling variations in handwriting styles and effectively analyzing expression structure and symbols. The proposed approach involves an iterative algorithm that exploits the interdependencies between symbol bracketing and structure analysis. By leveraging machine learning techniques, the system can provide soft interpretations with confidence valuesinstead of rigid outputs, thereby improving symbol identification and structure recognition.

III. RELATED WORK

Geofencing has become a common practice for many businesses due to the increasing popularity of mobile devices. Once a geographic region is identified, the potential applications for companies seem boundless, and it has found significant popularity in marketing and social media.

A. *Other Popular uses of Geofencing Include*

1) Social networking: Notably, Snapchat and other social networking applications use geofencing for location-based filters, stickers, and shared content. Users can apply promotional filters at events, create custom filters for special occasions, and contribute to public, location-based stories.
2) Marketing: Beyond social media, geofencing is widely used for in-store promotions, sending notifications to customers as they approach a shop. It is also used to target advertising to specific audiences based on their location data.[7]
3) Audience engagement: At events like concerts, festivals, and fairs, geofencing is employed to engage large audiences. Music venues can use geofencing to crowdsource social media posts or transmit event-related information.
4) Smart appliances: With the increasing prevalence of smart appliances equipped with Bluetooth capabilities, geofencing enables tasks like receiving alerts when running low on groceries or setting the thermostat to the right temperature when returning home from work.
5) Human resources: Some businesses use geofencing to track off-site field personnel, automating time cards and checking-in/out workers as they arrive and leave.
6) *Telematics:* Companies implement geofencing to create virtual zones around locations, workspaces, and secure areas in telematics. These zones can trigger alerts or warnings for drivers.
7) *Security:* Geofencing can be used to enhance mobile device security, such as enabling phones to unlock automatically when entering or leaving a designated area or receiving notifications when someone enters or leaves a property.
8) *Defense, Research, and Finance:* In critical sectors like finance, defense, and research, geo-fences can ensure that devices remain non-operational outside approved areas, safeguarding vital data and preventing unauthorized access.
9) *Delivery Executives:* Geofences can be assigned to specific delivery executives, ensuring efficient assignment of tasks and avoiding multiple deliveries to the same geographical area.[7]
10) *Schools:* Geofences on school-owned devices prevent students from taking them home and using them for personal gain, protecting the devices and enforcing their intended use for e-learning purposes.
11) *Fleet Management:* In logistics and transportation, geofencing helps track vehicle locations, ensuring prompt assistance in case of breakdowns and optimizing delivery routes to handle diversions or slowdowns.

By utilizing geofencing for diverse purposes, businesses can improve efficiency, security, and user experience across various domains.

Localization attacks focus on determining position and time information. Some examples follow.

• Sensitive place attacks (position attack): identifying important locations, such as home and work [15] [16].

IV. PROPOSED WORK

Geospatial Intelligence a Geo-fence is a feature that creates a virtual perimeter around a physical location. When a person enters or departs the boundaries of a certain region using a location-enabled device, actions are often triggered [3]. In most cases, the user will get a message with specific information that supports its real time position. The fundamental benefit of this technology is that it allows the virtual and real worlds to merge. We employ Geofencing in a number of initiatives, primarily in the health sector.

In this project proposal, we aim to introduce the authentication and authorization subsystems for Geo Server. We will explore various identity suppliers, including Geo fence borders, MAC (Media Access Control), and IP (Internet Protocol), while also providing examples of custom authentication plug-ins for Geo Server. Our objective is to integrate Geo Server into an existing security architecture. One of the key features we plan to implement is a virtual fence, which uses the global positioning system (GPS) to define geographical limits. To determine if a person is inside a geofence range, we will employ different methods such as Ray-casting, Winding Number, TWC (Triangle Weight Characterization), and Circular Geofencing utilizing the Haversine Formula. Whenever an individual enters or departs from a designated region, a geofence alert will be sent to the server. Additionally, if an attempt is made to access data outside of the geofence, our system will trigger the deletion of the corresponding files as a security measure. Furthermore, we will leverage geospatial intelligence technology, which utilizes GPS or RFID (radio frequency identification) to define geographical boundaries. This enables administrators to set up triggers that issue alerts when a device enters or exits the predefined boundaries. The virtual geofence barriers can be either active or passive in nature. In summary, this project proposal focuses on implementing Geo Server's authentication and authorization subsystems, exploring various identity suppliers, and integrating it into an existing security architecture. The introduction of a virtual fence and utilization of geospatial intelligence technology will enhance the system's security and monitoring capabilities.

Furthermore, we will leverage geospatial intelligence technology, which utilizes GPS or RFID (radio frequency identification) to define geographical boundaries. This enables administrators to set up triggers that issue alerts when a device enters or exits the predefined boundaries. The virtual geofence barriers can be either active or passive in nature.

In summary, this project proposal focuses on implementing Geo Server's authentication and authorization subsystems, exploring various identity suppliers, and integrating it into an existing security architecture. The introduction of a virtual fence and utilization of geospatial intelligence technology will enhance the system's security and monitoring capabilities.

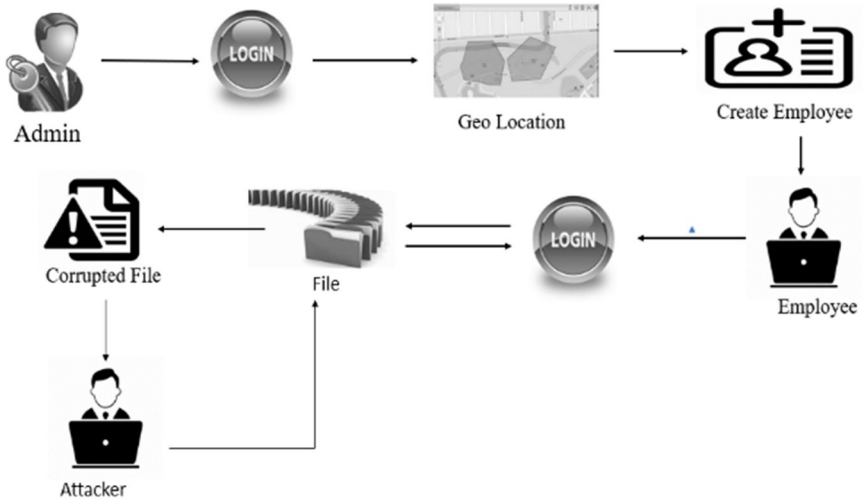


Fig .1. System Architecture

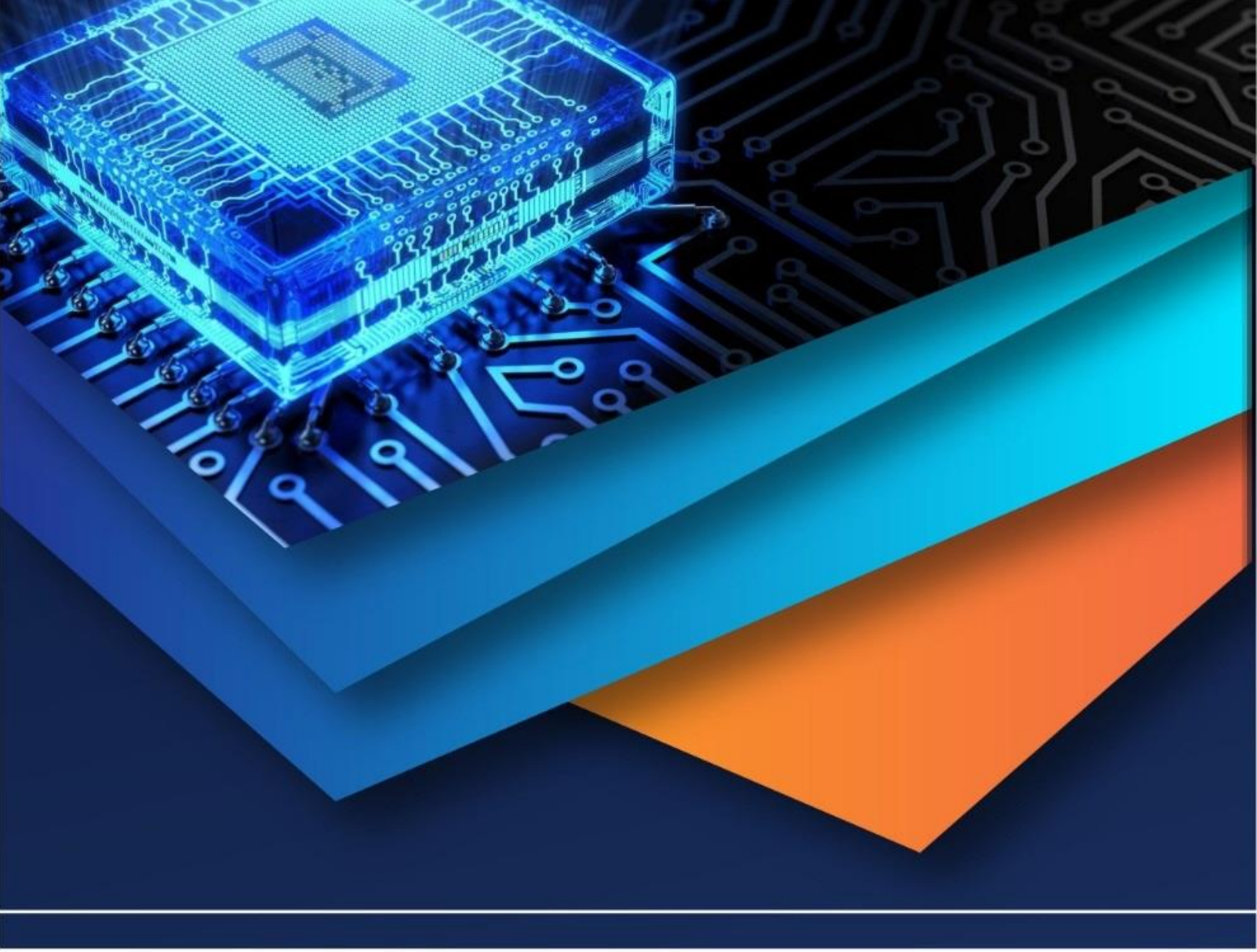
V. CONCLUSION AND FUTURE WORK

In this project, we developed a distinctive location-aware architecture for data security that ensures employees can participate while preserving their geographical privacy. Prior to employee engagement, we recognized the importance of implementing geo-fencing measures to ensure data privacy protection. We provided techniques and enhancements to efficiently select geo-fence zones with minimal overhead and a high job assignment rate. Additionally, the system automatically checks and verifies geo-fencing border values and the MAC Address. In case of any discrepancies, it triggers the erasure of victim files and the system to maintain data integrity.

In the future, we intend to incorporate more comprehensive regulations that encompass additional privacy considerations beyond just location data. We strongly advocate for the adoption of this strategy by prominent email service providers. However, caution must be exercised when implementing geofencing, particularly concerning marketing privacy. For instance, Massachusetts recently enacted consumer protection legislation, forbidding the use of location-based advertising. This legislation was passed only last year. A notable example is Copley Advertising, which faced legal action from the Attorney General for deploying geofences around women's health facilities to target women in waiting areas or nearby locations with anti-abortion commercial.

REFERENCES

[1] Rampérez, J. Soriano, D. Lizcano, and J. A. Lara, ``FLAS: A combination of proactive and reactive auto-scaling architecture for distributed services," Future Gener. Computer. Syst., vol. 118, pp. 56-72, May 2021.
[2] R. Mokadem and A. Hameurlain, ``A data replication strategy with tenant performance and provider economic prot guarantees in cloud data centers," J. Syst. Software., vol. 159, Jan. 2020, Art. no. 110447.
[3] Y. Mansouri, A. N. Toosi, and R. Buyya, ``Cost optimization for dynamic replication and migration of data in cloud data centers," IEEE Trans. Cloud Computer., vol. 7, no. 3, pp. 705718, Jul. 2019.
[4] A. E. Abdel Raouf, N. L. Badr, and M. F. Tolba, ``Dynamic data reallocation and replication over a cloud environment," Concurrency Comput., Pract. Exper., vol. 30, no. 13, Jan. 2018, Art. no. e4416.
[5] N. Mansouri, M. K. Rafsanjani, and M. M. Javidi, ``DPRS: A dynamic popularity aware replication strategy with parallel download scheme in cloud environments," Simul. Model. Pract. Theory, vol. 77, pp. 177-196, Sep. 2017.
[6] C. Liao, A. Squicciarini, and L. Dan, "Last-hdfs: Location-aware storage technique for hadoop distributed file system," in IEEE International Conference on Cloud Computing (CLOUD), 2016.
[7] Z. N. Peterson, M. Gondree, and R. Beverly, "A position paper on data sovereignty: The importance of geolocating data in the cloud." In HotCloud, 2011.
[8] J. Li, A. Squicciarini, D. Lin, S. Liang, and C. Jia, "Secloc: Securing location-sensitive storage in the cloud," in ACM symposium on access control models and technologies (SACMAT), 2015.
[9] A. Albeshri, C. Boyd, and J. G. Nieto, "Enhanced geoproof: improved geographic assurance for data in the cloud," International Journal of Information Security, vol. 13, no. 2, pp. 191–198, 2014.
[10] G. J. Watson, R. Safavi-Naini, M. Alimomeni, M. E. Locasto, and S. Narayan, "Lost: location based storage," in Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. ACM, 2012, pp. 59–70.
[11] Y. Mansouri and R. Buyya, ``To move or not to move: Cost optimization in a dual cloud-based storage architecture," J. Netw. Comput. Appl., vol. 75, pp. 223-235, Nov. 2016.
[12] R.Bharathi, T.Abirami," Energy efficient compressive sensing with predictive model for IoT based medical data transmission", Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z
[13] R.Bharathi, T.Abirami," Energy Efficient Clustering with Disease Diagnosis Model for IoT based Sustainable Healthcare Systems", Sustainable Computing: Informatics and Systems, 23 September 2020, https://doi.org/10.1016/j.suscom.2020.10045



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY