GeoBox: Data Loss Prevention System using Location Defined Network

R.Stalinbabu[1], R.Bharathi[2], L.Kanimozhi[3],V.Kiruthika[4],K.Naveen[5],M.Sangeetha[6]

[1,2] Assistant Professor,Department of Computer Science And Engineering,Cheran College Of Engineering,AnnaUniversity,Karur,Tamilnadu,India.

[3,4,5,6] U.G.Student,Department of Computer Science And Engineering,Cheran College Of Engineering,AnnaUniversity,Karur,Tamilnadu,India.

[1]Stalinbabucse@gmail.com,[2]bharathimkce@gmail.com,[3]kanimozhilogu2000@gmail.com,[4]kiruthikaccecse25@gmail.com, 5naveenk3401@gmail.com,

Abstract

These days, companies and organisations want the greatest data exchange and access capabilities. Remote working and mobile access to resources and collaboration platforms make data and resources more accessible from anywhere and at any time. Employees want to be able to access documents and email from a variety of devices and places at the same time. Businesses are constantly at risk from untrusted network access. This might lead to data loss and overexposure of sensitive information. To address the shortcomings of logical security mechanisms, security mechanisms that interact with the physical environment have been developed, which coincides with the development of cyber-physical systems. To protect the security of a company's data and resources. We propose an innovative Virtual Fence that leverages location data and geospatial intelligence in this project. Understanding, insight, decision-making, and prediction are all aided by geospatial data analysis. The visualisation and analysis of geographical data is used to obtain location intelligence (LI). Then, using the location-based cryptosystem, we strengthen the security of data access in Data Server for a firm or any other specified place. Within a company, Virtual Fence may be used to safeguard critical information. Off, On, Restricted View, or Read Only are the options. Once a geo-fenced border has been established, firms' options are only limited by their imagination. The key advantage of putting up a geo fence like this is that it prevents data leaking. No one can access data from a different network location/device after the trusted network locations have been specified. The experiment demonstrates that our approach can be used in real-world situations.

.

KEYWORDS: VirtualFence,GeospatialData,GeospatialIntelligence,Cryptosystem,GeoFence,Boundary Data Sharing,Security,Location Intelligence.

1. INTRODUCTION

The delivery of various services through the Internet is known as cloud computing. Data storage, servers, databases, networking, and software are examples of these resources, as illustrated in fig 1.1. 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. 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].

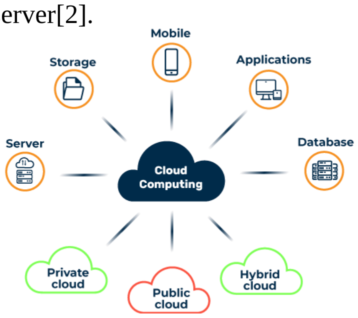


Figure 1.1. Cloud Services

1.1 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.

1.2 Geofencing

Geofencing is a location-based service in which a mobile device or RFID tag enters or departs a virtual boundary set up around a geographical area, known as a geofence[4], and an app or other software utilises GPS, RFID, Wi-Fi, or cellular data to trigger a pre-programmed action.

A geofence may activate mobile push notifications, trigger SMS messages or alerts, send targeted adverts on social media, monitor car fleets, block particular technologies, or offer location-based marketing data, depending on how it is designed.

Some geofences are used to monitor activity in secure zones, enabling management to get notifications when someone enters or exits the area[5]. Businesses may also utilisegeofencing to keep track of business property, monitor personnel in the field, and automate time cards.

1.3 How geofencing works

An administrator or developer must first create a virtual border around a specific area in GPS- or RFID-enabled software before using geofencing. When designing a smartphone app, this may be as easy as a circle drawn 100 feet around a place on Google Maps, as defined using APIs. When an authorised device enters or quits that region, the virtual geofence will trigger a reaction, as set by the administrator or developer..

2. RELATED WORK

Geofencing has been a regular practise for many firms as mobile devices have grown in popularity. Once a geographic region has been identified, the possibilities for what businesses may do appear limitless, and it has proven particularly popular in marketing and social media.

Other popular geofencing uses include:

- Social networking: Popular social networking applications, most notably Snapchat, are one of the most well-known uses for geofencing. Geofencing allows users to create location-based filters, stickers, and other shared content. It's all owing to these virtual perimeters, whether you're using a promotional filter at a concert, a custom-made filter for a friend's birthday, or posting to public, location-based stories.
- Marketing: Aside from social media, geofencing is a popular technique for companies to conduct in-store promotions by notifying you as you approach the shop. Businesses may also use geofencing to target advertising to a particular audience and determine which methods perform best based on user location data.
- Audience engagement: Geofencing is utilised to engage large audiences at events such as concerts, festivals, and fairs. A music venue, for example, may utilise a geofence to crowdsource social media postings or transmit venue or event information.
- Smart appliances: As more of our appliances become "smart," with Bluetooth capabilities, programming your fridge to warn you that you're out of milk the next time you pass by the grocery store is simpler than ever. You may also use a geofence to ensure that the thermostat is set to the right temperature when you arrive home from work.
- Human resources: Some businesses use geofencing to track personnel, particularly those who work off-site in the field. It's also a simple method to automate time cards, checking in and out workers as they arrive and go.
- Telematics: Companies may use geofencing to create virtual zones around locations, work spaces, and secure areas in telematics. They may be activated by a vehicle or a person, and they provide alerts or warnings to the driver.
- Security: Geofencing may seem intrusive, and it definitely has the ability to feel that way depending on how it's implemented. Geofencing, on the other hand, may be utilised to increase the security of your mobile device. You may, for example, arrange your phone to unlock when you enter or leave the house using a geofence, or to get notifications when someone enters or departs the property.
- Defence, Research, and Finance: IT may verify that devices deployed in finance, defence, or research are non-operational outside of the defined geo-fence by assigning geo-fences to them. IT may set different geofences for distinct regions of operation using an MDM application, and the device can become outdated outside of the geofences. The device is informed every time it enters or exits the geofence, allowing them to follow its whereabouts and check for any compliance issues. This keeps vital data on the device safe at all times and prevents access outside of approved areas.
- Delivery Executives: Assigning certain delivery executives to specific locations. By setting geo-fences to delivery executives, you may typically achieve maximum efficiency by avoiding having numerous delivery executives assigned to the same geographical region.

• Schools:E-learning is being increasingly widely used in schools to improve the training experience for college students. Setting geofences on school-owned devices removes the risk of pupils taking them home and exploiting them for personal gain. Geo-fences protect devices while also enforcing their intended use.

IT may implement numerous device restrictions for diverse geo-fences for remote and travelling employees. Wi-Fi setups and other settings particular to the business location are included in these device regulations. This allows employees to connect and work from numerous office locations without requiring IT assistance.

• Fleet Management: In logistics and transportation, devices with geo-fencing may assist in tracking the whereabouts of vehicles in the shortest amount of time. This guarantees prompt assistance in the event of a breakdown, as well as device and vehicle security. When diversions or slowdowns occur, geofencing is employed to aid the algorithm in making choices to redirect freight.

3.PROPOSED WORK

The Geo Server authentication and authorisation subsystems will be introduced in this project. Check out the many identity suppliers, such as Geo fence borders, MAC (Media Access Control), and IP (Internet Protocol), as well as offering examples of custom authentication plug-ins for Geo Server, integrating it into a home-grown security architecture. When data is tried to be opened outside of the geo fence, this system produces the victim file to wipe away the data..

3.1 Virtual Fence

The proposal calls for a Geo-fencing (geofencing) is a software feature that defines geographical limits using the global positioning system (GPS). Different methods, such as Ray-casting, Winding Number, TWC (Triangle Weight Characterization), and Circular Geofencing utilising the Haversine Formula, may be used to determine if a person is inside a geofence range. When someone enters or departs a certain region, a geofence alert is sent to the server. When data is tried to be opened outside of the geo fence, this system produces the victim file to wipe away the data.

3.2 Geospatial Intelligence Technology

Geo-fencing (geofencing) is a software feature that uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries. Geo-fencing allows an administrator to set up triggers so that an alert is issued when a device enters (or exits) the boundaries defined by the administrator. Virtual geofence barriers may be active or passive.

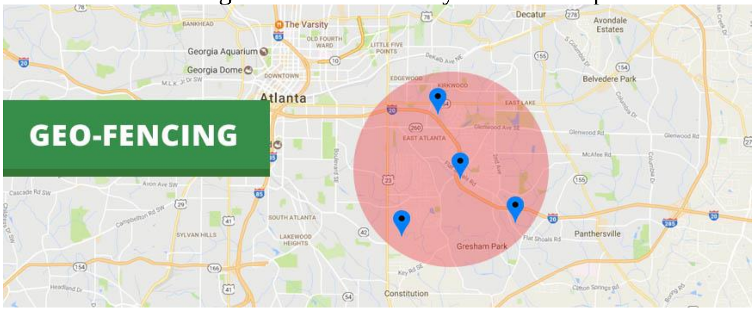
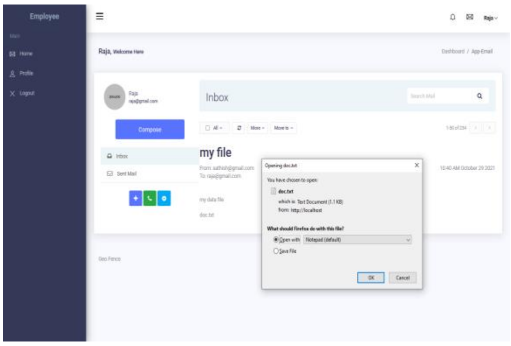


Figure .1.Geo-Fence Area

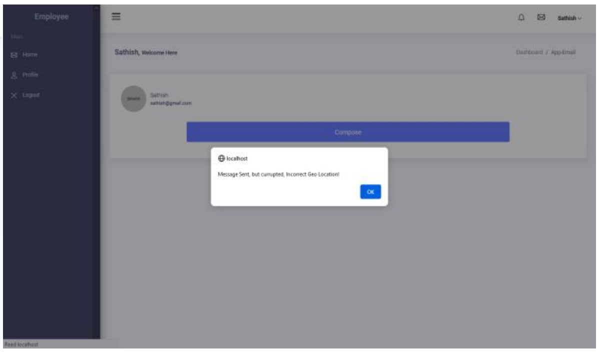
End users must opt-in to location services and have a mobile app open to utilise active geofences. Passive geofences are constantly on and function in the background, relying on Wi-Fi and cellular data instead of GPS or RFID. Geofences may be set up anywhere in the globe on mobile, tablet, and even desktop computers is shown in fig 1.

4. RESULTS AND DISCUSSION



my file
From: sathish@gmail.com
To: raja@gmail.com
10:40 AM October 29 2021
my data file
doc.txt

Opening doc.txt
You have chosen to open:
doc.txt
which is: Text Document (1.1 KB)
from: http://localhost
What should Firefox do with this file?
● Open with Notepad (default)
○ Save File
OK Cancel



localhost
Message Sent, but currupted, Incorrect Geo Location!

Fig..2. Geo fence corrupted data file Fig.3. Geo fence readable data file

This is a software feature that leverages the global positioning system to determine geographic boundaries. When data is tried to open outside of a geofence range, the system produces the victim file to wipe away the data displayed in fig.2. Scrap the system and data displayed in fig. 3.if you don't care about anything else.

5. CONCLUSION

We established a unique location-aware architecture for data security in this project, which allows employees to participate without compromising their geographical privacy. Before employees assent to a job, we identified geo fencing as a necessary step to guarantee that data privacy is safeguarded. We offered methods and improvements for selecting efficient geo fence zones with little overhead and a high job assignment rate. It also creates the victim files; it checks the geo-fencing border values automatically and wipes away the system and files if the geo-fencing and MAC Address are out of sync.

6. FUTURE WORK

We want to consider more elaborate regulations in the future to capture additional privacy considerations than location. We also advocate on using this strategy with prominent email service providers. Geofencing should be used with care, particularly when it comes to marketing privacy. Massachusetts was one of the first states to pass a consumer protection legislation prohibiting the use of location-based advertising only last year. Copley Advertising, which was contracted by a Christian group to put up a geofence around women's health facilities and target women in the waiting area or adjacent with anti-abortion commercials, was barred by the Attorney General.

7. REFERENCES

[1] V. Rampérez, J. Soriano, D. Lizcano, and J. A. Lara, ``FLAS: A combination of proactive and reactive auto-scaling architecture for distributed services," Future Gener. Comput. 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. Softw., 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 Comput., 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] N. Paladi and A. Michalas, "“one of our hosts in another country”: Challenges of data geolocation in cloud storage," in International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE), 2014, pp. 1–6.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12]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.

[13] 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

[14] 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.2020.100453