iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46319

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 10 Issue VIII August 2022- Available at www.ijraset.com

Virtual Fence Geospatial Intelligence to Protect Enterprise Cloud Server Data

S. Pandiaraj[1], Dr. J. Sreerambabu[2], D. Rajkumar[3]
[1]PG Scholar, [2]Head of the Department, [3]Assistant Professor Master of Computer Applications Department Thanthai Periyar Government Institute of Technology, Vellore -2

Abstract: ***Data sharing and access area unit capabilities businesses and organizations need the foremost currently. Remote operating and mobile access to resources and collaboration platforms created it easier to access knowledge and resources from anyplace, anytime. Employees need to access documents and email from completely different devices, and from varied locations at a time. Access from untrusted networks is usually a threat to businesses. This may lead to knowledge loss and overexposure of essential knowledge. To mitigate the deficiencies of logical security mechanisms, and coinciding with the trend of cyber-physical systems, security mechanisms are planned that integrate with the physical surroundings. to make sure that business's knowledge and resources area unit safe. In this project we tend to propose AN innovative Virtual Fence that uses a location knowledge and geospatial intelligence. Geospatial knowledge analysis enhances understanding, insight, decision-making, and prediction. Location intelligence (LI) is achieved via image and analysis of geospatial knowledge. Then we tend to improve the safety of information access in knowledge Server for an organization or the other specific locations exploitation the location-based cryptosystem. Virtual Fence provides a way to secure sensitive data among a company. It are often set to Off, On, Restricted read or browse solely. Once a geo-fenced boundary is outlined, the opportunities what businesses will do is proscribed by solely their creativeness. The most advantage of fitting such a geo fence is in avoiding knowledge discharge. Once outlined the trusty network locations, nobody will access knowledge from a unique network location/device. The experiment shows that our theme is possible in sensible applications.***

Keywords: Cloud service provider dashboard, Geo-fencing boundary fixing, Attacker Module, Victim File injection Whole, Wipe out system, performance evaluation.

I. INTRODUCTION

For a business, knowledge privacy transcends the PII of its customers and staff. It conjointly encompasses the data that helps it operate, whether or not it's conduct analysis and development knowledge or monetary info that shows however cash is spent at intervals the corporate. Recent history has shown that once knowledge that ought to stay personal gets into questionable hands, unhealthy things follow. Geofencing may be a location-based service within which associate degree app or different software system uses GPS, RFID, Wi-Fi or cellular knowledge to trigger a pre-programmed action once a mobile device or RFID tag enters or exits a virtual boundary created around a geographical location, referred to as a geofence. betting on however a geofence is organized it will prompt mobile push notifications, trigger text messages or alerts, send targeted advertisements on social media, permit pursuit on vehicle fleets, disable sure technology or deliver location-based selling knowledge. Some geofences square measure created to observe activity in secure areas, permitting management to visualize alerts once anyone enters or leaves a particular space. Businesses may use geofencing to observe staff within the field, automatise time cards and keep track of company property.

PURPOSE OF THE SYSTEM

The main purpose of the system is an company employee can't be accesses a file in own purpose it will be avoid them.

II. SYSTEM ANALYSIS

A. Existing System

Spatial-Temporal cradle Assurance with Mutual Proofs (STAMP) theme. STAMP is meant for ad-hoc mobile users generating location proofs for every alternative in an exceedingly distributed setting. However, it will simply accommodate trustworthy mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the situation proofs and protects users' privacy.

©IJRASET: All Rights are Reserved

A semi-trusted Certification Authority is employed to distribute science keys still as guard users against collusion by a light-weight entropy-based trust analysis approach.

1) *XAd:* This tool eliminates each style of assumption in promoting, as a result of it serves messages supported your potential consumer's location. xAd includes a proprietary platform that mechanically creates boundaries around places typically visited by a shopper. as an example, a eating house, shopping precinct. It's with these insights that marketers will target ads to their customers once they're at intervals those locations.
2) *Koupon Media:* This tool prompts a targeted provide to shoppers once they're at intervals the shop. Koupon Media has options that study the activity attribute of consumers at intervals the geofenced locations, and uses it to gift the client with offers they can't resist whereas they're looking.
   Ninth Decimal:
   This helps marketers to focus on customers close to their own stores or competitor's locations, with tangible media ads through phone calls, appointment requests, and couponing.
3) *Walmart:* It is another complete creating it real massive with geofencing. Their app comes with a store mode that picks up signals once a emptor is at intervals the shop, and delivers coupons and e-receipts.

B. Prposed System

This project can offer AN introduction to Geo Server own authentication and authorization subsystems.
like from basic/digest authentication and CAS support, check through the assorted identity suppliers, like Geo fence boundaries, mackintosh (Media Access Control), IP (Internet Protocol), similarly as providing samples of custom authentication plug-in for Geo Server, integration it in a very home-grown security design.
This technique creates the victim file for wipe out the info, once the info is tried to open outside of the geo fence.

1) *Virtual Fence*: The project propose a Geo-fencing (geofencing) may be a feature in a very software system program that uses the world positioning system (GPS) to outline geographical boundaries. To examine whether or not someone is at intervals a geofence vary we are able to build use of various algorithms like Ray-casting, Winding range, TWC (Triangle Weight Characterization) and Circular Geofencing victimisation Haversine Formula. Geofencing is security, once anyone enters or leaves a specific space, AN alert passes to server. This technique creates the victim file for wipe out the info, once the info is tried to open outside of the geo fence.
2) *Geospatial Intelligence Technology:* Geo-fencing is a feature in a software program that uses the global positioning system(GPS) or radio frequency identification(RFID) to define geospatial boundaries – fencing allow by the administrator to set up triggers so when a device enters (or exists) the boundaries defined by the administrator an alert is issued. Geofence virtual barriers can be active or passive.
   Active geofences require an end user to option to location services and a mobile app to open. Passive geofences are always on they rely on wi-fi and cellular data instead of GPS or RFID and work in background. Geofences can be set up on mobile, tablet and even desktop devices anywhere in the world.

III. DEVELOPMENT ENVIRONMENT

A. Hardware Specifications

1) Processor : Intel Corei3
2) Ram : 8GB
3) Hard Disk : 320GB

B. Software Specifications

1) Operating system : windows 10
2) Front-end : HTML, CSS, Bootstrap, Flask 1.1.1
3) Back-end : PHP
4) Server : WampServer 2i
5) Database : MySQL 5
6) Development tool : VS Code Editor

©IJRASET: All Rights are Reserved

IV. MODULE DESCRIPTION

A. Cloud Service Provider Dashboard

In this module we develop a cloud application, or cloud app, it is a software program where cloud-based and local components work together. This model relies on remote servers for processing logic that is accessed through a web browser with a continual internet connection. Cloud application servers typically are located in a remote data center operated by a third-party cloud services infrastructure provider. Cloud-based application tasks may encompass email, file storage and sharing. Third-party data sources and storage services can be accessed with an application programming interface (API). Cloud applications can be kept smaller by using APIs to hand data to applications or API-based back-end services for processing or analytics computations, with the results handed back to the cloud application. Vetted APIs impose passive consistency that can speed development and yield predictable results. Data stored on cloud services is instantly available to authorized users.

1) *Cloud Storage Server:* Cloud storage servers are virtual storage facilities provided by cloud service providers that help to store and access multiple files without the requirement of any direct physical device. Web storage server can be accessed via the internet. File Cloud offers the cloud storage in affordable cost and without any downtime. The cloud storage servers continuously run with the help of these data centers and are maintained by the cloud service providers. Data centers secure your files from any kind of damage and make those files available whenever you want to access it via the internet. Applications access cloud storage through traditional storage protocols or directly via an API. Many vendors offer complementary services designed to help collect, manage, secure and analyze data at massive scale. There are three types of cloud data storage: object storage, file storage, and block storage. Each offers their own advantages and has their own use cases:
2) *Object Storage:* Applications developed in the cloud often take advantage of object storage's vast scalability and metadata characteristics. Object storage solutions like Amazon Simple Storage Service (S3) are ideal for building modern applications from scratch that require scale and flexibility, and can also be used to import existing data stores for analytics, backup, or archive.File Storage - Some applications need to access shared files and require a file system. This type of storage is often supported with a Network Attached Storage (NAS) server. File storage solutions like Amazon Elastic File System (EFS) are ideal for use cases like large content repositories, development environments, media stores, or user home directories. Block Storage - Other enterprise applications like databases or ERP systems often require dedicated, low latency storage for each host. This is analogous to direct-attached storage (DAS) or a Storage Area Network (SAN). Block-based cloud storage solutions like Amazon Elastic Block Store (EBS) are provisioned with each virtual server and offer the ultra-low latency required for high performance workloads.
3) *Home Directories:* The use of home directories for storing files only accessible by specific users and groups is useful for many cloud workflows. Businesses that are looking to take advantage of the scalability and cost benefits of the cloud are extending access to home directories for many of their users. Since cloud file storage solutions adhere to required file system semantics and standard permissions models, customers can easily lift-and-shift applications to the cloud that need this capability.



B. Geo-fencing Boundary Fixing

Geo-fencing enables an executive to set up triggers so when a gadget enters (or leaves) the limits characterized by the chairman, an alarm are issued. Numerous geo-fencing applications consolidate Google Earth, enabling chairmen to characterize limits over a satellite perspective of a particular land territory.

C. Attacker Module

In Adversary module, the user can use the data on outside of the geo-fence area. It contains two types of attackers involves the system one is the attacker can be used an external device for copy the data in defense area, and another one is sending the data to the email. It is an one type of cyber-attacks, because an attempt to hackers to damage or destroy whole computer networks or system.

D. Victim File Injection Whole

In this module is used to automatically inject the malware file to the original file. The victim file, is perform the main role of our system, it is an .exe file format. Auto exe is automatically copying the external devices. Suppose the user attach file to the mail, it automatically converts the file to .zip format for preview blocking.

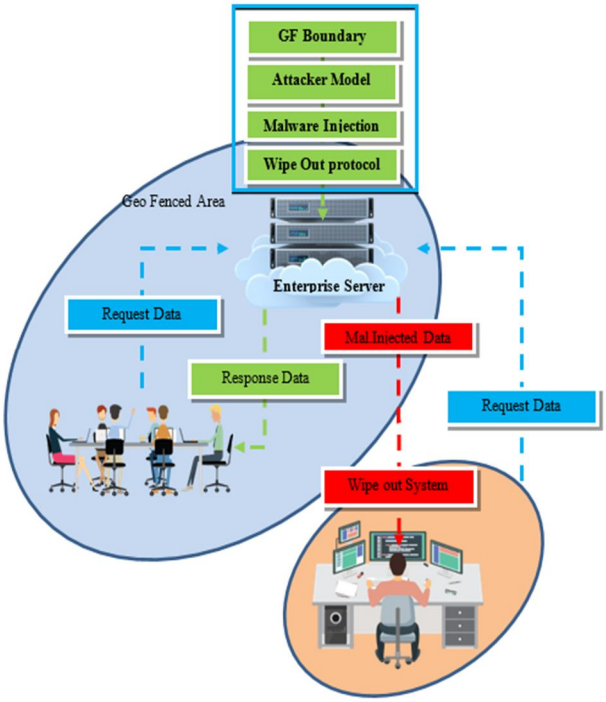
E. Wipe Out System

In the wipe out module, is wipeout the files and destroy the system when an exe find the system is adversary system. Auto exe is first checking the adversary system having internet connection, if it is having an internet connection, victim file reading the current system MAC, IP and Geo Location and compare with the server it doesn't match to send the adversary system information to the mail and wipeout the files and system. Otherwise, it does not care of anything scrap the system and data.

F. Performance Evaluation

A geo- fencing system is usually used for location-based service. First time we will use the data security in defense. This system provides the more security for an essential data.

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

In this project, we introduced a novel location-aware framework for provide data security, which enables the participation of workers without compromising their location privacy. We identified geo fencing as a needed step to ensure that data privacy is protected prior to workers consenting to a task. We provided heuristics and optimizations for determining effective geo fencing regions that achieve high task assignment rate with low overhead. It also generates the victim files; it automatically checks the geo - fencing boundary values and wipeout the system and files when geo - fencing and MAC Address is mismatch.

VII. FUTURE ENHANCEMENT

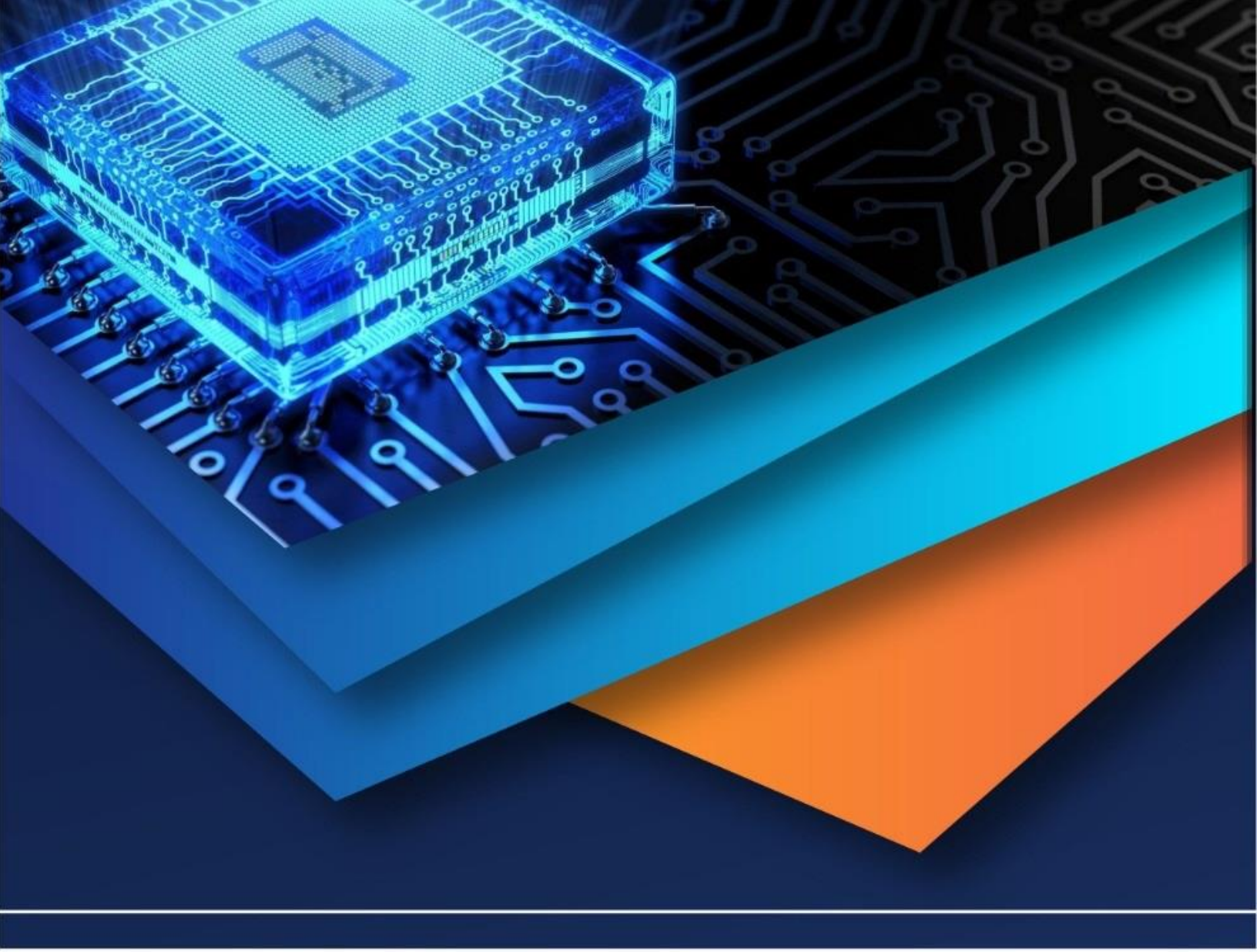
In the future, we plan to take into account more complicated policies to capture other privacy requirements other than the location. And also we insists this method to popular E-Mail Service Provider too.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

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.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)