IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁒ Impact Factor 8.102 ⁒ Peer-reviewed / Refereed journal ⁒ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12536

Data Loss Prevention System Using Location-Defined Network

Ms.R. Indumathy[1] G. Priyadharshini [2], C. Shruthi[3], R. Senbagavalli Madhumitha[4]

[1], Assistant Professor, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India

[2]B.E, Department of Computer Science and Engineering, DMI College of Engineering, Chennai, India

[3]B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

[4]B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India

Abstract-Data sharing and access are capabilities businesses and organizations require the most these days. Remote working and mobile access to resources and collaboration platforms made it easier to access data and resources from anywhere, anytime. Employees want to access documents and emails from different devices and from various locations at a time. Access from untrusted networks is always a threat to businesses. This might result in data loss and overexposure of critical data. To mitigate the deficiencies of logical security mechanisms, and coincide with the trend of cyber-physical systems, security mechanisms have been proposed that integrate with the physical environment. To ensure that the business's data and resources are safe. In this project, we propose an innovative Virtual Fence that uses location data and geospatial intelligence. Geospatial data analysis enhances understanding, insight, decision-making, and prediction. Location intelligence is achieved via visualization and analysis of geospatial data. Then we improve the security of data access in the Data Server for a company or any other specific location using the location-based cryptosystem. Virtual Fence provides a means to secure sensitive information within an organization. It can be set to Off, On, Restricted View, or Read Only. Once a geo-fenced boundary is defined, the opportunities that businesses can do is limited by only their creativity. The main benefit of setting up such a geo fence is in avoiding data leakage. Once defined the trusted network locations, no one can access data from a different network location/device.

Keywords: virtual fence, Location intelligence, cloud computing, geospatial data, cyber-physical systemI

I INTRODUCTION

A. Overview

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Cloud computing can be both public and private. Public cloud services provide their services over the Internet for a fee. Private cloud services, on the other hand, only provide services to a certain number of people. These services are a system of networks that supply hosted services. There is also a hybrid option, which combines elements of both public and private services. Cloud Computing is a combination of the use of computer technology (computing) and Internet-based development (cloud) Cloud is a metaphor for the internet, as is the cloud that is often depicted in computer network diagrams. Cloud computing is a general concept of other recent technological trends that are widely known to include SaaS and Web 2.0 with the general theme of being dependent on the Internet to provide users with computing needs. For example, Google Apps provides general business applications online that are accessed through a web browser with software and data stored on the server. Cloud Computing is also an abstraction of the complex infrastructure that is hidden. It is a computational method in which information technology-related capabilities are presented as a service, so that users can access them via the Internet without knowing what is inside, being expert with them, or having control over the technological infrastructure that helps them.

B. Problems Identified

The advantages of cloud computing are frequently touted as cost-efficient, reliable, manageable, and more secure than legacy computing.

Yet cloud computing possesses security risks despite it being more secure than legacy computing. And the security disadvantages of cloud computing remain

worrisome. Most cloud service providers implement relevant security standards and industry certifications to ensure that their cloud environment remains safe. However, storing data and business-critical files in virtual data centers can potentially open you up to risks.

C. Unexpected but Most Serious Security Risk: World experience shows that internal security risks began to prevail over external ones. Now the main source of threats to the company's IT systems is not hackers or malware at all, but the company's employees. Leaks can be caused both by unintentional, erroneous actions, and deliberate wrecking by staff. For example, it could be selling information to competitors, seizing confidential information, or sabotaging administrative security policies. This trend is confirmed by numerous studies around the world.

D. Loss of Control: The enterprise's loss of control in enhancing the network's security is the most significant disadvantage of cloud computing security. The responsibility of securing the network is shared between the cloud service provider (CSP) and the enterprise. Depending on which server model an enterprise uses, the enterprise may have little to almost no control over cloud security. Infrastructure-as-a-Service (IaaS) allows the enterprise to have the most control as the CSP only provides the infrastructure. It falls under the enterprise's jurisdiction to build the remainder of the stack and maintain its security. A stack built, operated, and managed entirely by the CSP is known as the cloud service offering, Software-as-a-Service (SaaS). The enterprise has the least amount of control over cloud security in a SaaS environment. Enterprises need to review the CSP's service level agreement (SLA) to understand its security obligations and to identify gaps in security coverage.

E. Vendor Lock-in: Describes the "an anticipated fear of difficulty in switching from one alternative to another." Lock-in often happens when enterprises neglect to read the CSP's SLA.
Data Loss: This can occur via a natural disaster or company error.

Insider Theft: When an employee intentionally steals data with mal-intent. Vulnerability to attack: In cloud computing, every component is online, which exposes potential vulnerabilities. Even the best teams suffer severe attacks and security breaches from time to time. Since cloud computing is built as a public service, it's easy to run before you learn to walk. After all, no one at a cloud vendor checks your administration skills before granting you an account: all it takes to get started is generally a valid credit card.

F. Data Breaches: Force Point lists the consequences of data breaches in the cloud in its white paper, "Deploying and Managing Security in the Cloud." It states that "while cloud providers generally have better security capabilities than most organizations and suffer fewer data breaches as a result, a successful data breach can open an organization to stiff financial penalties, regulatory fines, loss of customer confidence, and declining competitive market positioning, among other significant consequences."

G. Unsecured Application Programming Interfaces (APIs):

The open APIs are readily exploitable as "CSPs expose a set of application programming interfaces (APIs) that customers use to manage and interact with cloud services (also known as the management plane)."

H. Geospatial Intelligence

A Geo-fence is a feature that defines a virtual boundary around a real-world geographic area. Every time the user enters or exits the boundary of a particular area, actions are often triggered during a location-enabled device. Usually, the user will receive a notification with certain information that supported its location in real-time. The main advantage of this technology is that it creates a fusion between the virtual world and the real one. We make use of Geo fencing in several projects, particularly within the health industry.

II. LITERATURE SURVEY

Ivan Gaidarski; Pavlin Kutinchev 21-22 November 2019: The paper presents our approach to protecting sensitive data, using the methods of Big Data. To effectively protect the valuable information within the organization, the following steps are needed: Employing a holistic approach for data classification, identifying sensitive data of the organization, identifying critical exit points -

DOI: 10.17148/IJARCCE.2023.12536

communication channels, applications, and connected devices and protecting the sensitive data by controlling the critical exit points. Our approach is based on creating of component-based architecture framework for ISS, conceptual models for data protection, and implementation with COTS IT security products as Data Leak Prevention (DLP) solutions. Our approach is data-centric, which is holistic by its nature to protect the meaningful data of the organization.

Bhavya Singh Shishodia; Manisha J. Nene: 25-27 November 2022: Transferring both allowed and illegitimate information is increasingly routine. This increased the potential danger to sensitive information and opened the door to further threats. A data breach is becoming commonplace in the headlines. All kinds of harm may be done with stolen information. A Data Leakage Prevention System (DLPS) is a scheme for preventing the unauthorized release of sensitive information inside an organization's internal network. The purpose of this study is to investigate different strategies for data security and the effects of preventing data leaks. Objective notes were taken on installation procedures and issues encountered. The deployment of industrial Data Leakage Prevention solutions in major organizations to safeguard cyber data has also been highlighted. The study holds the potential

to guide the way toward the implementation of technical solutions to handle the challenges envisaged in the ever-evolving environment, benefiting both academics and professionals.

Mohammed Ghouse; Manisha J. Nene; VembuSelvi C. 20-21 December 2019: Data leakage in an organization is a very important concern that leads to the ex-filtration of data, The work in this paper addresses a novel concept for the prevention of data leakage for data in transit. The text under consideration is classified into confidential or non-confidential categories based on the content and context using the Machine Learning technique. Subsequent action for encryption is performed on the confidential data and then transmitted from the Intranet domain to the Internet domain ensuring that the data is not compromised by unauthorized users. In addition, normal transactional data which is not confidential in nature is not prevented from transmitting and is easily accessible by a third party. Encryption is applied only to selected data and not the entire data in transit, ensuring that the hardware resources are efficiently utilized. An adversary can simply compose an e-mail with the organization's confidential information as the body of the mail, in such scenarios, our method will classify the e-mail content and will encrypt the data so that the data is not revealed to an outsider.

Marc Lemercier; Lyes Khoukhi 10-12 October 2022: The vehicle ad-hoc network (VANET) is a promising technology that enables numerous vehicular network applications to improve road safety, navigation, and many other purposes. Android Automotive supports many applications for vehicles. Each application has a list of accesses, called permissions, required for specific interfaces or sensitive data. However, some applications request permissions unrelated to functionalities or unnecessary permissions. Furthermore, they improperly collect user data. Given the privacy risk associated with applications, it is necessary to study the permissions requested by the application before installation. A permission system is a solution to deal with abusive applications. However, such a system suffers from limitations as users may ignore it during the installation phase due to the complexity of understanding the permissions. This article proposes a graph-based model to determine abusive applications by automatically analyzing the requested permissions. This aims to build a confidence indicator to choose applications with more respect for privacy. This model would inform the user about the possibility of data leakage risks by assigning a privacy score.

Jing Ma; Yonggang Xu; Jinqiang Fan; Xiaobin Yao; Yaming Cao; Chen Zheng 22-24 October 2022: Electric power is an important basic industry related to the development of the national economy and social stability, and once the data of the power industry is leaked, it may cause serious damage to the legitimate rights and interests of power users and enterprises, as well as social order and public interests. With the introduction of relevant laws and regulations in the field of data security, data security supervision has become stricter, and in the context of the construction of new power systems, the demand for open data sharing in the power industry will increase significantly, and the compliance processing data of power enterprises will face a severe test. This paper focuses on the risk of data leakage in the power industry, proposes a data-centered security protection model, combines the characteristics of the power industry, designs the data leakage prevention scheme of the power industry based on the model, and gives deployment implementation suggestions.

III.PROPOSED SYSTEM

This project will provide an introduction to Geo Server's own authentication and authorization subsystems. such as from basic/digest authentication and CAS support, check through the various identity providers, such as Geo fence boundaries, MAC (Media Access Control), IP (Internet Protocol), as well as providing examples of custom authentication plug-ins for Geo Server, integrating it in a home-grown security architecture. This system creates the victim file to wipe out the data when the data is attempted to open outside of the geo fence.

A. Virtual Fence

The project proposes a Geo-fencing (geo-fencing) feature in a software program that uses the global positioning system (GPS) to define geographical boundaries. To check whether a person is within a geo-fence range we can make use of different algorithms such as Ray-casting, Winding Number, TWC (Triangle Weight Characterization), and Circular Geo fencing using the Haversian Formula. Geo-fencing is security, when anyone enters or leaves a particular area, an alert passes to the server. This system creates the victim file to wipe out the data when the data is attempted to open outside of the geo fence.

DOI: 10.17148/IJARCCE.2023.12536

B. Geospatial-Intelligence Technology

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

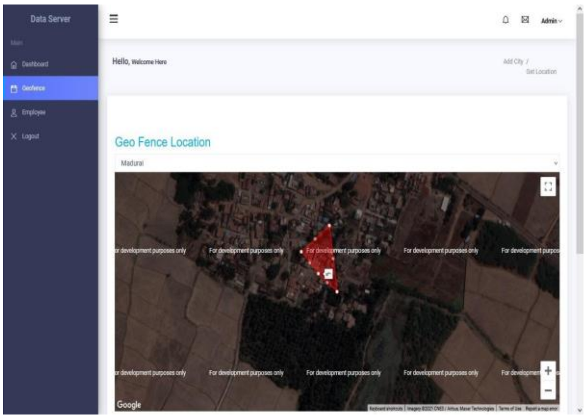
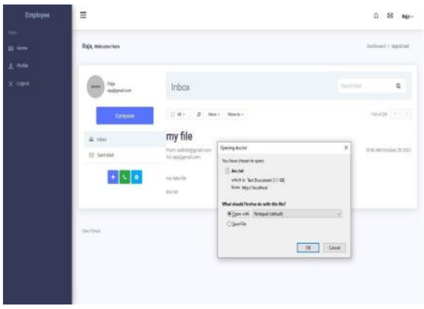


Figure 1: Creating Geo fence location

Active geo fences require an end user to opt-in to location services and a mobile app to be open. Passive geo fences are always on; they rely on Wi-Fi and cellular data instead of GPS or RFID and work in the background. Geo fences can be set up on mobile, tablet, and even desktop devices anywhere in the world.



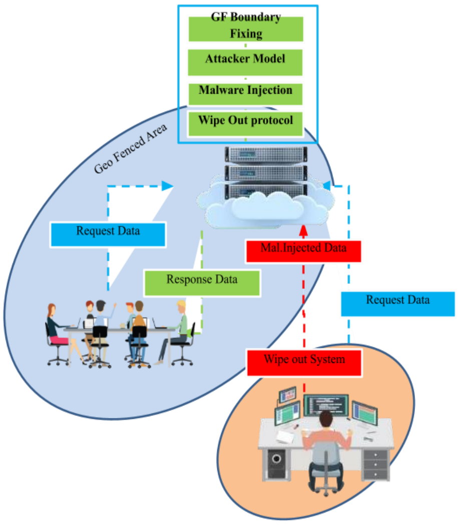


Figure 2: System Architecture

IV. RESULTS AND DISCUSSION

DOI: 10.17148/IJARCCE.2023.12536

We have built a project which has shown promising results. Customers can use our software to build a defense around their data. This data that is being protected by our software cannot be hacked or tampered with. The user can also access this data from any corner of the world.

CONCLUSION

In this project, we introduced a novel location-aware framework for providing 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 before workers consent to a task. We provided heuristics and optimizations for determining effective geo-fencing regions that achieve high task assignment rates with low overhead. It also generates the victim files; it automatically checks the geo-fencing boundary values and wipeout the system and files when geofencing and MAC Address is mismatched.

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. 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.

4. 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.

5. 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.

6. 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.

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. AL Beshri, C. Boyd, and J. G. Nieto, "Enhanced proof: 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.