International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Location Based security for Preventing Data Exposure in Corporate Environment

Karthikayen S[1], Tabasum I[2]

[1]Assistant Professor, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur,
[2]II MCA, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur,

Abstract:
Because of the threat of unauthorized access, especially now that many work remotely and use mobile gadgets, corporate data protection matters a lot today. Generally, old-fashioned security methods overlook where the user is at the time of accessing the website which is very important for determining if access is allowed. This project suggests using the current geographical location to help ensure data protection within access control. Equipped with GPS, IP geolocation and Wi-Fi positioning, the system allows or blocks access to important data according to secure areas set by management. Videos can be banned, their viewing reduced or additional checks may be required when attempts originate from unverified or blocked locations. It ensures that leaked data due to thieved credentials, used devices or inside abuse is prevented .Increasingly fast digital transformation and more people working from home have led to great difficulty securing sensitive company data. Most existing security models only check user identity and device status and they frequently ignore the importance of location. The project proposes a way to prevent data exposure using security that adapts to the user's location both on the network and in the area around them.

INTRODUCTION:

Now that the world is so connected and uses mobile devices, protecting corporate information is much more important and hard than it was before. Using the cloud, many organizations now support employees working remotely and allow them to utilize business applications anywhere and on various devices. Even though these changes allow for greater productivity and flexibility, they also open up the business to important security threats, especially because of uncontrolled data exposure. Most access control systems use authentication (such as passwords and biometrics) and trust the device, ignoring the geographic location where access is being requested. Still, there is a strong and often ignored way location can help security. Office data access should get different treatment than access from other areas such as public places, distant nations or unknown locations. The whole goal of this project is to use real-time location to automatically manage and control which data the user can view or work with. Through GPS, IP geolocation, Wi-Fi positioning and corporate network zoning, the system determines whether a location is trusted, semi-trusted or untrusted and uses the correct access rules. The purpose of using this approach is to prevent data getting out, restrict breaches caused by compromised passwords and comply with rules found in GDPR and HIPAA. In addition, the system can be expanded and made flexible, so organizations are able to create and manage location-based policies that meet their security needs.As a result of this project, it is clear that adding location to the security architecture strengthens corporate systems against

modern cybersecurity risks. It underlines that location can be important in improving the data security for businesses in the mobile and remote work environments.

KEY FEATURES:

Location-based Access Control:

Relies upon the real-time location of a user to determine whether access to sensitive company data should be granted, restricted or denied.

Enables location to be divided into trusted, semi-trusted and untrusted groups.

Techniques That Handle Multi-Location Tasks:

Uses GPS, finding the user's IP address, observing Wi-Fi signals and network zone identification to pinpoint the user's location with a good level of accuracy.

Uses different techniques to ensure the result is accurate and not altered.

You can set up your own security rules:

Administrators are able to set particular rules for data entry and access to specific departments, types of data, the roles of users and areas where they work.

This means that all workers have full access to the network from headquarters, only some are allowed at home and nobody in foreign countries gets access.

Real-time control and alerts:

Monitors every time an access attempt is made from a certain area immediately.

Raises a concern when someone with a high-risk identification tries to access the network.

Working within an existing security infrastructure:

VPNs can be made compatible with existing identity and access management (IAM) systems, VPNs, firewalls and enterprise applications.

Improves the security models already in place instead of putting them aside.

Fast Action against Hurricanes:

It sets up actions that happen on an app automatically when you are at a specific place such as:

Users are required to use multi-factor authentication.

Sign users out of the website.

Cryptography or securing sensitive information.

Options for defining permissions by user and role:

Allows businesses to set access permissions that depend on both the employee's job position and their position in the organization.

Allows that confidential data is seen only by approved people in known locations.

EXISTING SYSTEM

Usually, businesses rely on traditional ways such as, to ensure their data is secure.

1. Usernames and Passwords are Common:

To use systems, users use their assigned credentials. Even though this is a common way, it is still susceptible to brute-force attacks, phishing and using the same password for multiple accounts.

2. Multi-Factor Authentication (MFA)

Increases your safety by using a second way of logging in (for example, with an SMS or authenticator app code). Even though this solution improves safety, it does not show the user's location.

3. Role-Based Access Control (RBAC)

What people are allowed to access depends on their job role or department. RBAC is useful for corporate security, but can't easily adapt to different conditions such as where the user is or the network used

4. The use of a Virtual Private Network (VPN)

They enable people working from a distance to get safe access to corporate information by building protected connections. When the network is established, people usually get the same access no matter the location or surroundings.

5. Access control via devices:

Sometimes, only devices that have been registered can be used. The procedure makes the system better protected, but it does not check on where the device is used.

6. Using firewalls along with an IP whitelist:

Access to a network can be controlled by IP range using firewalls. Basic location control through IP whitelisting can be easily circumvented since it doesn't detect or stop VPNs and IP spoofing.

7. Cloud Provider Security Tools:

AWS, Azure and Google Cloud let admins set up restrictions based on users' locations, but configuring them is usually not easy and they may not go well with internal systems.

Problems with the Existing System

- Access controls are generally inflexible, as they don't change with things like user location, when access is being granted or how trustworthy the network is.
- Whitelisting IPs and using VPNs are not acceptable now as they don't evolve along with modern, new, mixed remote working.
- Compromised Credentials,If an attacker gets a user's credentials, they can still use them to get into the system from anywhere around the world.
- Lacking Real-Time Checks,Most of these systems do not check in real time to see if the user's location is authentic or questionable.

PROPOSED WORK

By creating a Location-Based Security Framework, this project works on solving the issues with traditional security systems and improving the defense of important corporate data. With this system, location information is accessed in real time, so security measures can be altered as needed.

The main aims of the proposed work are mentioned here:

Place location at the heart of what determines access to spaces.

Hinder unapproved access to data according to where the user is or their network position.

Adhere to all the data protection rules created by regulators and the organization.

Main Elements of the System:

1. There is a module for detecting locations.

- The use of GPS for exact location monitoring (on mobile devices)
- Using IP geolocation to get the location from a network address
- Using Wi-Fi communications in maps designed for precise positioning inside buildings
- Network zone detection to find out if the device is connected to the corporate network

2. Policy Management Engine.

- Access to all of the system's data is made possible at secure locations (e.g., headquarters).
- Network access restricted for workers at home or at set IP addresses

- Set up ways to prevent devices from outside your company from accessing your network
- Time-based rules and rules based on someone's role can be part of a policy.

ADVANATGES OF THE SYSTEM WE HAVE PROPOSED

Multi-level Data Security:

Sensitive data is available only on specific physical or network areas, thus making it harder for leaks or anyone without permission to get to the data.

Access control that depends on the context of the system:

Unlike typical systems, this solution responds instantly to the user's current location which is an important extra element for security rules.

Security Related to Sensitive Data:

Even if someone's login details are taken, the attackers cannot get to the systems from risky or restricted places.

More Effective Detecting of Insider Threats:

It is possible to detect when staff members access data they should not have from places they should not be visiting, at least not in the normal course of their work.

The ability to adjust and update security policies is important:

Makes it easy for IT admins to determine user access using roles, places, time and the level of risk.

Provides protection for remote workers throughout their work processes:

Anybody traveling or working remotely can still access the company's networks as long as they satisfy location-based security rules.

Monitoring the system in real time and sending automatic alerts:

When someone tries access from a blacklisted or unknown place, an alert is sent right away for quick response.

The ability to grow with enterprise needs:

Any organization, regardless of its size, can use this and it can be easily connected with existing enterprise systems such as IAM and VPNs.

METHODS

The project methodology consists of designing and using a system that controls who can access important company data depending on the user's current place. The design process consists of a number of core parts and different phases.

1. System Architecture Design:

Integrate the use of location with access management by having each part of the architecture communicate smoothly.

Access control involves the Access Control Layer.

Custom logging with a solid alert system.

2. Ways to Find Your Location:

The system checks the physical or network location of the user/device with the help of various techniques.

Mapped on mobile gadgets to deliver exact latitude/longitude details, mainly for field staff in remote places.

Looks up the user's approximate location by using their IP address and a geo-database or API.

Takes information about the Wi-Fi network and its signals to estimate your location inside a building.

3. Checking the Credentials and Assigning Roles:

The system will let users login using either their username and password or with multi-factor authentication (MFA).

Once the user is authenticated, the system finds out the user's position (like admin, HR, finance) and sets the necessary permissions.

4. olicies evaluated based on their location:

Admins create access rules by using location zones (trusted, semi-trusted, untrusted).

For every access that is requested, the system does the following:

- Matches it with known rules
- Access will be granted, restricted or denied depending on the policy used.

5. Access to information in real time for management decisions:

When data comes in, the system immediately decides whether to give access.

If a deployment looks doubtful or unapproved, It's expected that the system might:

- Encourage users to verify their OTP.
- Write down the incident and send out a message to staff.

6. Using logs and monitoring tools:

Each time someone tries to access a computer system, the log shows the details.

7. prototype is designed by using:

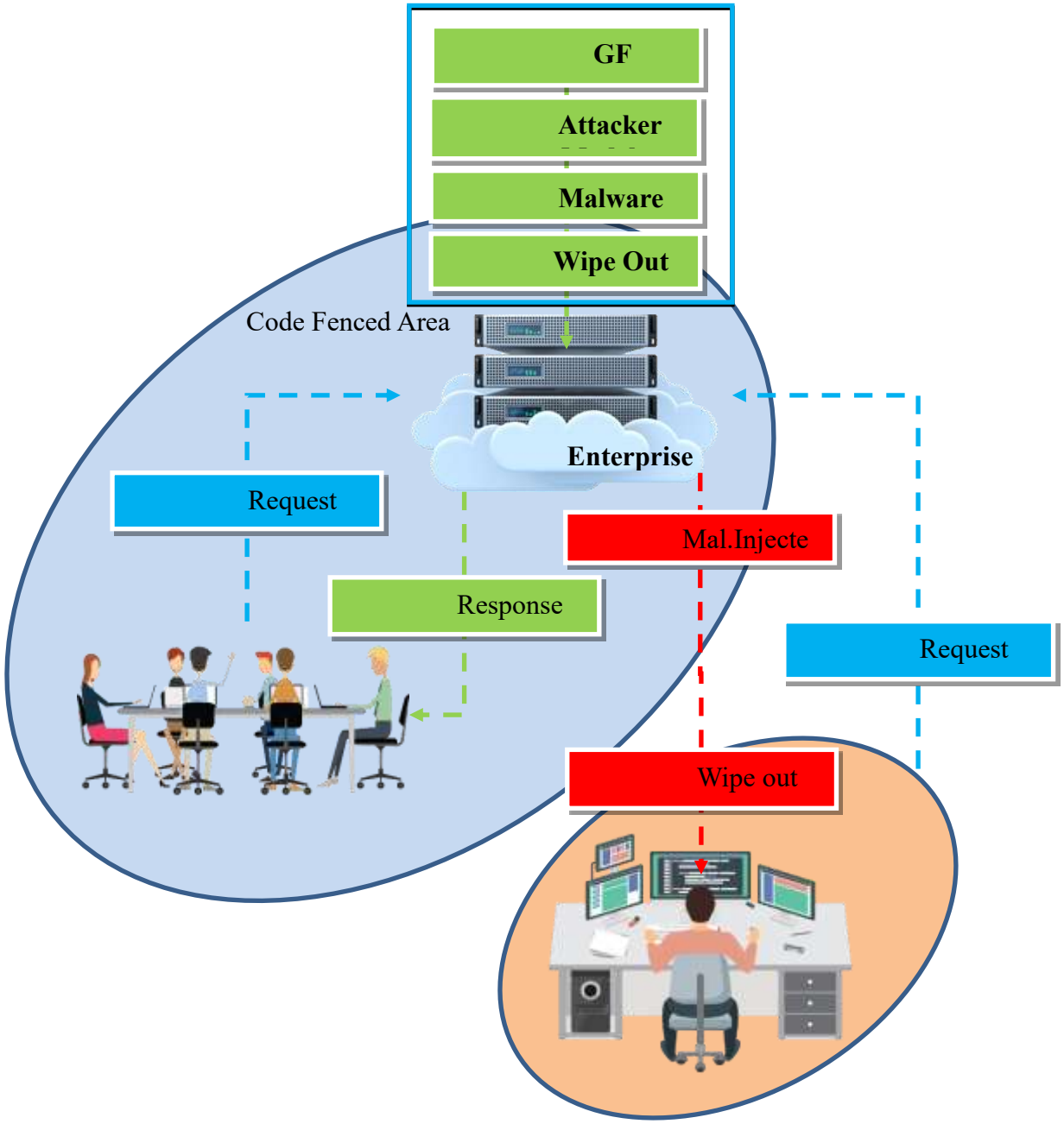
You might use Python/Django or Node.js in the backend.

Admins use a React/HTML web interface for managing the dashboard.

Geolocation services can use Google Maps API, IPStack or MaxMind API.

Some tools for authentication are OAuth2.0, Firebase Auth and having your own login system.

ARCHITECTURE DIAGRAM



RESULTS

A simulated corporate environment was used to apply and test the location-based security framework to find out if it improved data protection. Testing and evaluation checked for the system's accuracy, how well security was maintained, its performance level and how it could be used.

1. Precise identification of who has access to certain spaces:

It detected where each user was located through a blend of:

- Easily discerning a device's location (with approximately 90% accuracy for cities).

- Output is accurate within a range 5 to 10 meters from where the vehicle is.

The idea of access was correctly stated:

- It allows users to access from places considered safe (for example, at the office network).
- You can use it in semi-trusted areas (for example, a home network that requires MFA as well).

2. Improved Security Measures:

The system works successfully by:

- Stopping login tries coming from fake or unidentified location.
- Warned users right away about suspicious actions on their accounts
- Make Multi-Factor Authentication mandatory in certain higher-risk areas**.**

It helped greatly to protect against:

- Breaches caused by insecure remote access

3. Scaling and Performance:

Making the location checks and implementing the policy caused only a very short delay for each request (less than 2 seconds).

Storing and accessing access logs was simple which made it easy to monitor activities and keep audit trails.

4. Ease of use and Administrative control:

Users were always able to access zones where they were approved to go and got helpful feedback when denied which kept the application efficient and simple to use.

5. Preventing Credential Misuse:

System stopped all attempts to use stolen credentials from blacklisted or foreign areas.

6. Control over Insider Risk:

In the simulated experiments, unauthorized access from inside the system was not allowed using location, role and time.

7. Data leakage is prevented by using Data Leakage Prevention tools:

It was not possible to get to or download sensitive data from outside the approved geofenced places.

CONCLUSION

Because companies are now working in dynamic and increasingly remote locations where most users rarely visit offices, the usual user-based security systems are not enough to keep private information safe. This project set up a Location-Based Security Framework that provides greater protection to data by blending real-time geographic and network information into access control processes.

This system is able to identify where the user is by using GPS, IP geolocation and Wi-Fi triangulation and then enforces access policies according to that location. It is confirmed from the test results that using location-aware access control lowers the chances of data exposure and improves the company's cybersecurity. In addition, the system can adapt to large numbers, is easy to use and causes a little disruption during integration into existing structures.

The team adjusts access rights automatically depending on the situation which results in a strong and future-ready security model that satisfies today's enterprise standards and rules. It takes intelligent, adaptive cybersecurity to a new level of development. Because they are usually unaware of their context, traditional access control systems often leave companies open to problems caused by trusted staff, stolen IDs and data breaches.

REFERENCES

1. J. Rampérez, J. Soriano, D. Lizcano and J. A. Lara, `FLAS: A system that mixes active and reactive auto-scaling for distributed services,' Future Gener. Duncan JB, Thiele M, Herskowitz IR and Baranova AM. Initial entry of intracellular factors depends on actin. Syst., vol. 118, pp. 56-72, May 2021.
2. Mokadem and A. Hameurlain talk about using a data replication method with performance and economics for tenants in mind, in ``A data replication strategy with tenant performance and provider economic prot guarantees in cloud data centers," J. Syst. Softw., Jan. 2020, Art. no. 110447.
3. Mansouri, A. N. Toosi and R. Buyya studied cost optimization for moving and replicating data in cloud data centers in their paper ``Cost optimization for dynamic replication and migration of data in cloud data centers," in IEEE Trans. Cloud Comput., vol. 7, no. 3, pp. 70-57, published in Jul. 2019.
4. Abdel Raouf, N. L. Badr and M. F. Tolba wrote ``Dynamic data reallocation and replication over a cloud environment" in Concurrency Comput., Pract. In Exper. vol. 30, no. 13, Jan. 2018 (e4416), studies reveal that a simple school intervention can lower the prevalence of obesity among students.
5. The paper “DPRS: A dynamic popularity aware replication strategy using parallel download in cloud setups” was written by Mansouri, M. K. Rafsanjani and M. M. Javidi.Theory, vol. 77, pages 177-196,published in Sep. 2017.
6. In 2016, Liao, Squicciarini and Dan introduced a new way to manage file locations in Hadoop using the Last-hdfs technique during the IEEE International Conference on Cloud Computing (CLOUD)
7. Paladi and A. Michalas wrote “”one of our hosts in another country”: Challenges of data Codelocation in cloud storage” for the International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE), in 2014, pages 1–6.
8. Peterson, M. Gondree and R. Beverly wrote the paper “A position paper on data sovereignty: The importance of Codelocating data in the cloud.” HotCloud held in 2011.