WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Email Server Data Protection System using Geo-fence Framework and Decision Tree Algorithm

Manikandan[1], Sivasurya[2], Varun kumar[3], Prof Ranjani[4]

[1]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: manikandancse57@gmail.com
[2]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: sivasuryapgm@gmail.com
[3]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: k.varunkumar124@gmail.com
[4]Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: ranjani@egspec.org

A B S T R A C T

Email is one of the mostly used method for exchanging messages.It is also used for both individual and organizational uses. The sent data has the potential to be hacked.Therefore, this email server data protection system, which uses Geo-fence technology and adecision tree algorithm is used to securely transfer data.Geo-fence framework is used for both Watermarking and Encryption to share active content.A geo-fence is a virtual barrier that encircles a physical location.A Geo-fence could be created dynamically as a radius around a spot.A watermarking technique is used to hide information on digital assets, such as photographs, documents, and videos. For data security, encryption techniques are used.Encrypted information is protected from illegal access and reading by using encryption.Finally, using the entered data entry process, the authorized user can extract the encryption key. When the user information does not match the embedded information, unauthorized access can be discovered. This application helps to track unauthorized access and prevent the distribution of content in the email environment. It also, provides group data sharing based on legal process using adecision tree algorithm and provides approval for the post delivery system.If any unauthorized access to the information is discovered, a notification of the forgery will be sent to the administrator.

Keywords:Geo-fence framework, Encryption, Watermarking,Decision tree algorithm

1. INTRODUCTION

Email is an open and accessible one. It allows people in organizations to communicate with each other and with people in other organizations. The problem is that email is not secure.As a result, attackers can utilize email to cause issues in order to profit. Attackers use email to steal sensitive information since most businesses rely on it to do business. Because email is an open format, anyone who can intercept it can read it, posing a security risk. As businesses began sending confidential or sensitive information via email, this created a problem. There is software that can sniff Internet packets for data like system passwords and confidential documents. On a network, attackers utilize this programme to access confidential data and attachments. As a result, the information's secrecy, and authentication may be mistreated. The provision of appropriate security measures against unauthorized data disclosure and manipulation is known as information and communication technology (ICT) security. It is linked to privacy since unsecured information cannot protect consumers' privacy. A system's ability to maintain I anonymity, II sender authenticity, III message integrity, IV non-repudiation, and V consistency. Email exchanges can be characterized as secure. Email authentication is the most effective technical approach for demonstrating that an email

* Varun kumar.Phone.no:+919344193661.
E-mail address: k.varunkumar124@gmail.com

is genuine. In other words, it allows you to verify that an email originates from the person who claims to be the sender. Email authentication is most commonly used to prevent fraudulent email activities like phishing and spam

2. METHODOLOGY

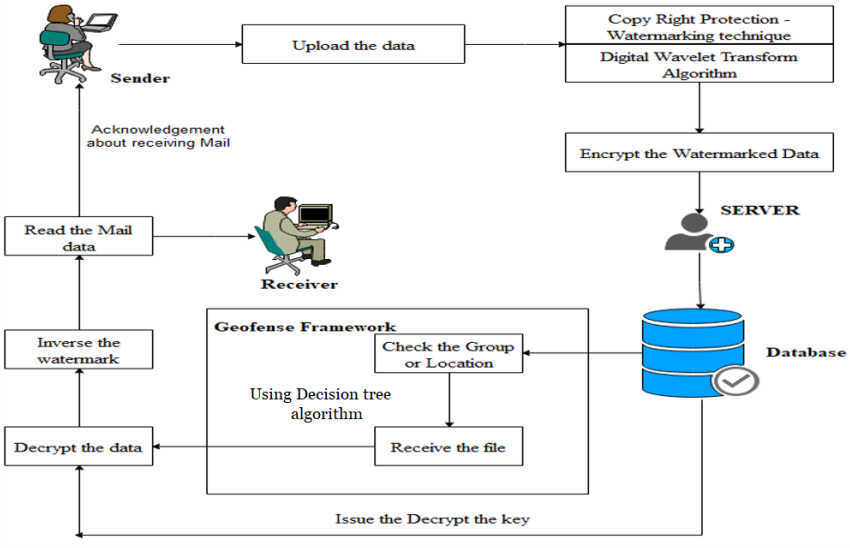
First, in this email server data protection system, users must register their personal information, username, and password. The data thus collected will be saved in a database. From this, only authorized persons will be allowed to sign in using their username and password. After that, users can start exchanging data with others using the email server data protection system. The data is then watermarked and encrypted in the geo-fence framework before being distributed to others. For watermarking, the discrete wavelet transform (DWT) method is used because it provides the best visual quality in images. For encryption, the AES encryption (Block cipher) method is used. The sender will select the media files such as documents, videos, and photos to be transmitted and send them to a specified person or group.The data is both watermarked and encrypted in the geo-fence framework and stored in the database before it is passed on to others.The data thus transmitted will only be sent to the person or group that was previously collected in the database.The decision tree algorithm is used to select a specific person or group and share the data and decryption key. It guides the data and decryption key to reach a specific person or group. If the person or group needs to view that data, they must ask the sender for the decryption key using the key request.The sender will examine the key request and send the hidden decryption key to the individual or group via media files such as images, documents, and videos. Finally, the person or group can view the data by entering the correct decryption key.And also, in this email server data protection system, the sender may also know that the sent data has been viewed by the person or group. All these activities will be recorded in the database. The administrator can view these activities at any time using the database.

In this email server data protection system, the below methods are used:

- Geo-fence framework
- Discrete wavelet transform (DWT)
- AES encryption (Block cipher)
- Decision tree algorithm

3.MODELING AND ANALYSIS

Our aim is to create an email server data protection system that incorporates both the geo-fence framework and the decision tree algorithm. Geo-fence technology includes both watermarking and encryption. The watermarking protects the original data and prevents data redistribution, and encryption prevents unauthorized viewing or access. The decision tree algorithm is used to select a specific person or group and share the data and decryption key. It guides the data and decryption key to reach a specific person or group. All these activities are stored in the database.The below figure 1 illustrates the data transfer process of the email server data protection system.



Objective

Figure 1. The data transfer process of the Email Server Data Protection System

- Creating a reliable and secure framework for data exchange.
- The content provider or sender can determine who can access or view the data and also prevent the data redistribution.
- Provides the alert system at the time of unauthorized system access.

4. RESULTS AND DISCUSSION

1. Email is an open and accessible medium, and most businesses rely on it to do business.
2. As a result, attackers can utilize email to steal sensitive information.
3. By intercepting an email, an attacker might readily access or view its contents.
4. As a result, the information's secrecy, and authentication may be mistreated.

Proposed System

The data transmitted in this proposed system is encrypted and watermarked using the geo-fence framework. The decision tree algorithm is then used to select the specific person or group. This prevents unauthorized data access and redistribution. If any unauthorized access to the information is discovered, a notification of the forgery will be sent to the administrator.This leads to secure communication and data transmission between the sender and receiver.

Use Case Diagram

The below figure2describes the data flow ofthe email server data protection system.

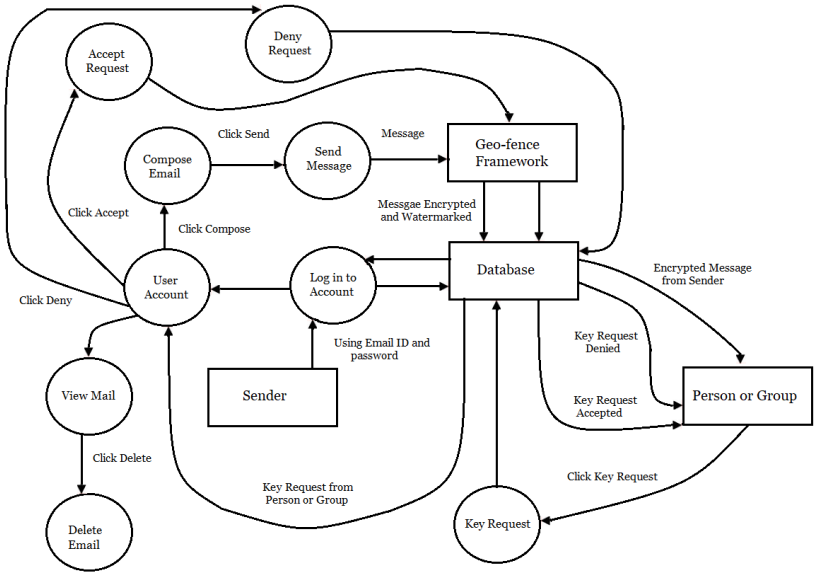


Figure 2. Data flow of email server data protection system

Algorithm

DECISION TREE ALGORITHM

The decision tree algorithm is used to select a specific person or group and share the data and decryption key. It guides the data and decryption key to reach a specific person or group.

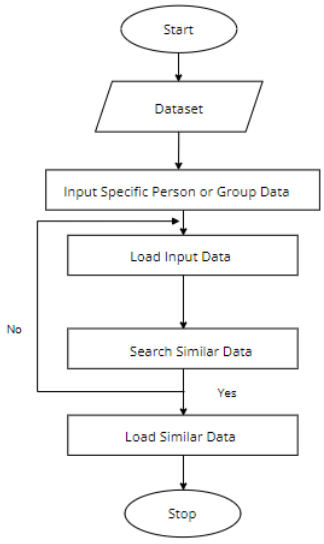


Figure 3. Process of selecting a specific person or group for data transfer

CONCLUSION

E-mail is a widely used and complicated internet application. It is an open and accessible one, so, by intercepting an email, an attacker might readily access its contents. As a result, it is necessary to provide security in the email system. The data transmitted in this proposed system is encrypted and watermarked. So, this prevents unauthorized data access and redistribution. And also, if any unauthorized access to the information is discovered, a notification of the forgery will be sent to the administrator. This will lead to preventing such unauthorized access in the future. This enables secure communication and data transmission between the sender and receiver.

REFERENCES

[1]. Sandro Rodriguez Garzon and Bersant Deva, "Geofencing 2.0: taking location-based notifications to the next level", *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2014.

[2]. Yan Xiao and Guangyong Gao, "Digital watermark-based independent individual certification scheme in wsns", *IEEE Access*, vol. 7, pp. 145516-145523, 2019.

[3].Osama Hosam and Muhammad Hammad Ahmad, "Hybrid design for cloud data security using combination of AES ECC and LSB steganography", *International Journal of Computational Science and Engineering*, vol. 19, no. 2, pp. 153-161, 2019.

[4]. Vinod Kumar, Musheer Ahmad and Pankaj Kumar, "An identity-based authentication framework for big data security", *Proceedings of 2nd International Conference on Communication Computing and Networking*, 2019.

[5]. Dilip Venkata Kumar Vengala, D. Kavitha and AP Siva Kumar, "Three factor authentication system with modified ECC based secured data transfer: untrusted cloud environment", *Complex & Intelligent Systems*, pp. 1-14, 2021.

[6]. Minal Barapatre and C. N. Deshmukh, Design & Development of Network Geo-Fencing Model for User Monitoring and it's Alertness in a Security Applications.

[7]. Heba Abdul-Jaleel Al-Asady, Osama Qasim Jumah Al-Thahab and Saad S. Hreshee, "Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper" in Journal of Physics: Conference Series, IOP Publishing, vol. 1818, no. 1, 2021.

[8]. Eugene Bagdasaryan et al., "Ancile: Enhancing privacy for ubiquitous computing with use-based privacy", *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, 2019.

[9]. E. S. Hureib and Adnan A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography and image steganography", *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)*, vol. 20, no. 8, pp. 1-8, 2020.

[10].Imran Ahmad Khan and Rosheen Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptography", *International Journal of Computing and Communication Networks*, vol. 1, no. 1, pp. 46-52, 2019.

[11]. Saša Pešić et al., "Gemat-internet of things solution for indoor security geofencing", *Proceedings of the 9th Balkan Conference on Informatics*, 2019.

[12]. Jiaxing Xuan et al., "Design of secure and independent controllable email system based on Identity-Based Cryptography", *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016.