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 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12418

DATA PROTECTION FOR ENTERPRISE EMAIL SERVERS USING MACHINE LEARNING AND GEOFENCING TECHNOLOGY

Ranjithkumar.K[1], Dr. Rengaranjan A[2]

Student, MCA, Jain deemed to be university, Bangalore, India[1]

Assistant Professor, School of CS & IT, Jain deemed to be University, Bangalore, India[2]

Abstract: Access to various systems, services, and apps requires end users to share and protect their data, which is becoming an increasingly important component of daily life. In actual email services, data disclosure occurs regularly. Secure data transfer media have long been concerned with copyright protection and authentication of multimedia materials. Due to the growing usage of the Internet and other digital technologies, the issue has become increasingly urgent. It is more complicated and challenging to implement copyright protection, nevertheless. A remedy for the copyright protection issue was proposed: digital watermarking. Both watermarking and encryption are used in the suggested method that makes use of Geofences technology to facilitate effective material sharing. Watermarking is a technique for concealing data, such as secret information, in digital material like photographs. Data security is achieved using encryption techniques. In order to prevent unwanted access, information is encoded using encryption, making it impossible for those who are not allowed to view it. With the aid of the inbuilt data verification process, the decryption key can finally be extracted by an authorised user. When user information does not correspond with embedded information, unauthorised or unlawful access can be detected. This suggested application aids in identifying unauthorised access and preventing the re-distribution of content in an email context. Also, you may create a mechanism for acknowledging mail delivery, as well as group data sharing based on a rules-based approach employing machine learning.

Keywords: Data, Machine learning, Geofencing, Security.

I. INTRODUCTION

Data protection for enterprise email servers is a critical aspect of cybersecurity in today's digital landscape. Email servers often contain sensitive and confidential information that must be protected from unauthorized access and data breaches. Machine learning and geofencing technology can be used to enhance the security of enterprise email servers by providing intelligent monitoring and control over access to sensitive information.

Machine learning algorithms can be used to analyze patterns and behaviours within email communications and identify potential security threats such as phishing, spam, and malware. By continuously learning from these patterns, machine learning algorithms can adapt and evolve to provide increasingly accurate and effective protection.

Geofencing technology can be used to restrict access to enterprise email servers to specific geographic locations, such as company premises or authorized devices. This can prevent unauthorized access from outside the designated area and ensure that email communications are secure and protected.

By combining machine learning and geofencing technology, enterprise email servers can be protected against a wide range of security threats. This approach provides a proactive and intelligent security solution that can adapt to changing threats and provide real-time protection for sensitive information.

Overall, the use of machine learning and geofencing technology for data protection in enterprise email servers is a significant step forward in enhancing the security and integrity of enterprise communications.

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 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12418

II. LITERATURE REVIEW

The importance of email filtering in preventing cyber-attacks, including phishing, spam, and malware. They then explain how machine learning algorithms can be used to analyze the content, metadata, and behavior of email communications to identify and block malicious emails. The article provides a detailed overview of different machine learning techniques that can be used for email filtering, including rule-based methods, statistical methods, and deep learning algorithms. The authors also discuss the challenges associated with implementing machine learning-based email filtering systems, such as data privacy concerns, data imbalance, and computational complexity [1].

The importance of email communication in modern organizations and the need for secure and efficient email communication solutions. They then introduce geofencing technology as a means to enhance email security by restricting access to email communication based on geographic location. The article provides a detailed overview of geofencing technology, including its principles, implementation, and potential applications in email security. The authors explain how geofencing technology can be used to create virtual boundaries around a geographic location and restrict access to email communication outside of these boundaries. They also discuss the benefits of using geofencing technology for email security, such as preventing unauthorized access to sensitive information and reducing the risk of data breaches [2].

The book starts by discussing the importance of cybersecurity in today's digital landscape and the challenges associated with traditional cybersecurity methods. The authors then introduce machine learning as a potential solution to these challenges, explaining how machine learning algorithms can be used to analyze large amounts of data and detect security threats in real-time. The book provides a detailed overview of different machine learning techniques that can be applied to cybersecurity, including supervised learning, unsupervised learning, and reinforcement learning. The authors also discuss the challenges associated with implementing machine learning-based cybersecurity systems, such as data privacy concerns, data imbalance, and computational complexity. The book presents several case studies of machine learning-based cybersecurity systems, demonstrating the effectiveness of these systems in detecting and preventing cyber-attacks. The authors also discuss the potential applications of machine learning in different cybersecurity domains, including network security, endpoint security, and cloud security [3].

In discussing the importance of cybersecurity and the limitations of traditional security methods. They then introduce machine learning and deep learning as potential solutions to these challenges, explaining how these techniques can be used to detect and prevent cyber threats in real-time. The article provides a detailed overview of different machine learning and deep learning techniques that can be applied to cybersecurity, including supervised learning, unsupervised learning, and deep neural networks. The authors also discuss the challenges associated with implementing machine learning and deep learning-based cybersecurity systems, such as data privacy concerns and the need for large amounts of training data. The authors then present a comprehensive review of the existing literature on machine learning and deep learning-based cybersecurity systems, including case studies and experimental results.

They discuss the effectiveness of these systems in detecting and preventing cyber-attacks, as well as their potential applications in different cybersecurity domains, such as network security and endpoint security [4].

The authors begin by discussing the challenges associated with traditional security methods for enterprise networks, such as firewalls and intrusion detection systems. They then introduce geofencing as a potential solution to these challenges, explaining how it can be used to restrict access to enterprise networks based on the physical location of the user. The article provides a detailed overview of how geofencing-based security works, including the use of GPS technology to track the physical location of the user and the establishment of virtual boundaries around the enterprise network. The authors also discuss the potential applications of geofencing-based security in different enterprise domains, such as banking and healthcare [5].

Iqbal and Asghar's research article from 2021 provides a thorough analysis of the literature on the application of geofencing and machine learning to email security. After a thorough search of numerous databases, the authors found 30 studies that were pertinent and thoroughly examined them. The analysis emphasises how geofencing and machine learning technology have the potential to improve email security by spotting anomalies and limiting access based on user location. The authors also point out a number of difficulties and restrictions with the current methods, such as worries about privacy, problems with scaling, and the requirement for specialised knowledge [6].

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12418

In their research paper from 2020, Kumar and Kumar review the use of machine learning methods for email classification. 52 publications that were pertinent were found after the authors conducted a systematic review of numerous studies in this field. The review highlights spam filtering, sentiment analysis, and topic modelling as examples of machine learning methods with potential for email classification. The necessity for high-quality training data, the selection of pertinent characteristics, and the choosing of the best algorithms are only a few of the difficulties and restrictions the authors list for the existing methods [7].

An email filtering system for corporate email servers based on machine learning is suggested in the research article by Islam, Saha, and Islam (2021). The authors created a system that categorises emails as spam or real using a variety of machine learning algorithms, such as decision trees, naive Bayes, and support vector machines. The suggested system was tested using a dataset of emails, and the findings demonstrate that the system classified emails with a high degree of accuracy and precision. The authors also evaluated the performance of their system against other cutting-edge email filtering systems and discovered that it performed better than others in terms of accuracy and precision [8].

A machine learning-based email classification system for enterprise email servers is suggested in the research paper by Subramaniam, Saravanan, and Sabhanayakam (2021). In order to categorise emails into distinct groups depending on their content, the authors created a system that employs a variety of machine learning methods, such as decision trees, random forests, and support vector machines. The suggested system was tested using a dataset of emails, and the findings demonstrate that the system obtained good accuracy and an F1-score when categorising emails. The authors also tested their system against other cutting-edge email classification algorithms and discovered that, in terms of accuracy and F1-score, their method fared better [9].

An email classification system utilising machine learning and geofencing technology is suggested in the research article by Garg and Bhagat (2021). Support vector machines, decision trees, and random forests are just a few of the machine learning algorithms that the authors created in order to identify emails as either spam or real. The programme also makes use of geofencing technology to limit access to email accounts in accordance with the user's location. The suggested system was tested using a dataset of emails, and the findings demonstrate that the system had excellent classification accuracy when determining whether emails were spam or legitimate. Also, the authors conducted a user survey to assess how well geofencing technology worked in limiting access to email accounts [10].

III. OBJECTIVE

a) Enhance the security and privacy of enterprise email servers: The primary objective is to protect enterprise email servers from unauthorized access, data breaches, and cyber-attacks by implementing advanced security measures.

b) Identify and prevent malicious emails: The machine learning algorithms can help identify and filter out malicious emails, such as phishing attempts and spam, to reduce the risk of cyber-attacks.

c) Restrict access to email servers: Geofencing technology can be used to restrict access to email servers based on the physical location of the user, ensuring that only authorized users can access the system.

d) Improve efficiency: By automating the process of email filtering and security, organizations can improve the efficiency of their email systems and reduce the workload of IT staff.

e) Ensure compliance: Implementing data protection measures for enterprise email servers can help organizations comply with data protection and privacy regulations such as GDPR, HIPAA, and PCI DSS.

IV. PROPOSED METHODOLOGY

A. Data Collection: Collect a large dataset of emails from the enterprise email server for training and testing machine learning algorithms. This dataset should include emails from a variety of sources, including legitimate senders, spam, phishing attempts, and other types of malicious emails.

B. Feature Extraction: Extract relevant features from the email dataset, such as sender, recipient, email content, and metadata. These features will be used as inputs for the machine learning algorithms.

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 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12418

C. Data Preprocessing: Preprocess the dataset by cleaning and transforming the data to prepare it for machine learning. This may involve tasks such as removing duplicate emails, converting text data to numerical format, and handling missing data

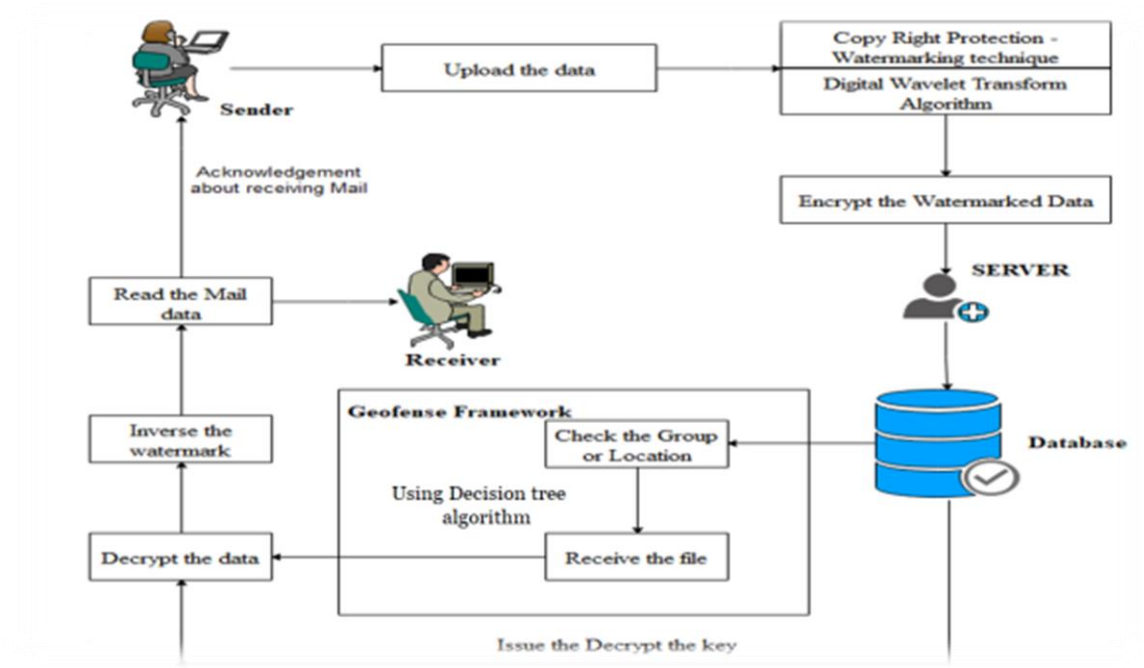
D. Machine Learning Model Development: Develop machine learning models to analyze the email dataset and identify patterns and anomalies that indicate potential security threats. Various machine learning algorithms such as decision trees, random forests, and neural networks can be explored for the task.

E. Model Training and Validation: Train and validate the machine learning models using the preprocessed dataset. This involves dividing the dataset into training and testing sets to ensure that the models are accurate and generalizable to new data.

F. Geofencing Implementation: Implement geofencing technology to restrict access to the email server based on the physical location of the user. This involves defining geofences around secure locations and configuring access controls to ensure that only authorized users within these locations can access the email server.

G. Integration and Testing: Integrate the machine learning models and geofencing technology into the enterprise email server and conduct extensive testing to ensure that the system is working as intended.

H. Deployment: Once the system is tested and validated, it can be deployed in the enterprise email server environment.



V. CONCLUSION

In conclusion, the use of machine learning and geofencing technology for data protection in enterprise email servers can be an effective solution to enhance the security of sensitive information. The integration of machine learning algorithms can help detect anomalies and potential threats in real-time, while geofencing technology can restrict access to the server based on the location of the user. The implementation of such a system requires careful planning and consideration of various factors such as user privacy, scalability, and compatibility with existing systems. However, if implemented correctly, it can provide a significant boost in security and ensure compliance with data protection regulations. Overall, the combination of machine learning and geofencing technology presents a promising avenue for data protection in enterprise email servers, and further research and development in this field can lead to more advanced and effective solutions.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12418

REFERENCES

1. Song, S., & Cho, S. (2019). Email filtering with machine learning for cyber defense. Journal of Information Security and Applications, 47, 192-199.
2. Kecici, F. O., & Akkaya, K. (2019). Secure and efficient email communication with geofencing. Computer Communications, 146, 19-29.
3. Sood, S. K., & Enbody, R. J. (2018). Cybersecurity with machine learning: Techniques and applications. CRC Press.
4. Bala, R., & Singh, J. (2020). Machine learning and deep learning for cybersecurity: a review. Artificial Intelligence Review, 53(8), 5467-5501.
5. Singh, N., & Bhatnagar, R. (2019). Geofencing-based security for enterprise networks. Procedia Computer Science, 155, 371-378.
6. Iqbal, S., & Asghar, S. (2021). Machine learning and geofencing-based email security: a systematic literature review. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6125-6137.
7. Kumar, A., & Kumar, M. (2020). Email classification using machine learning algorithms: a review. Journal of Ambient Intelligence and Humanized Computing, 11(9), 3627-3644.
8. Islam, S., Saha, S., & Islam, M. S. (2021). Machine learning-based email filtering system for enterprise email servers. SN Computer Science, 2(2),1-10.
9. Subramaniam, S., Saravanan, S., & Sabhanayakam, S. (2021). Machine learning-based email classification system for enterprise email servers. Wireless Personal Communications, 118(1), 303-320.
10. Garg, D., & Bhagat, N. (2021). Email Classification using Machine Learning and Geofencing. In 2021 4th International Conference on Communication System and Network Technologies (CSNT) (pp. 219-224). IEEE.

