Enterprise Email Server Data Protection System Using Geo-Fence Technology And Machine Learning

Sowmiya SR[1], PraveenKumar P[2], SivakandanP[3],Vigneshwaran A[4], Vinothkumar D[5]
[1, 2, 3, 4, 5] Dept of CSE
[1, 2, 3, 4, 5]Dhanalakshmi Srinivasan Engineering College,Perambalur,TN,INDIA

Abstract- *Data sharing and Protection are increasingly becoming an essential part of the daily life for end users to access different systems, services, and applications. Data disclosure frequently occurs in real-world E-mail services. Authentication and copyright protection of multimedia contents has always been a concern in secure data transfer media. In proposed approach using Geofens technology both Watermarking and Encryption approach utilized for efficient content sharing. Watermarking is used to hiding the information such as hide secret information in digital media like images. Encryption techniques used to provide security to data. In encryption, the information is encoding to prevent unauthorized access and the unauthorized persons cannot read it. Finally, authorized user can extract decryption key with the help of embedded data verification process. Big data refers to the large, diverse sets of information that grow at ever-increasing rates. It encompasses the volume of information, the velocity or speed at which it is created and collected, and the variety or scope of the data points being covered (known as the "three v's" of big data). Big data often comes from data mining and arrives in multiple formats.*

Keywords- Data Protection,Geo Fence Technology and Machine Learning.

I. INTRODUCTION

Big data refers to the large, diverse sets of information that grow at ever-increasing rates. It encompasses the volume of information, the velocity or speed at which it is created and collected, and the variety or scope of the data points being covered (known as the "three v's" of big data). Big data often comes from data mining and arrives in multiple formats. Big data can be categorized as unstructured or structured. Structured data consists of information already managed by the organization in databases and spreadsheets; it is frequently numeric in nature. Unstructured data is information that is unorganized and does not fall into a predetermined model or format. It includes data gathered from social media sources, which help institutions gather information on customer needs. Big data can be collected from publicly shared comments on social networks and websites, voluntarily gathered from personal electronics and apps, through questionnaires, product purchases, and electronic check-ins. The presence of sensors and other inputs in smart devices allows for data to be gathered across a broad spectrum of situations and circumstances. Big data is most often stored in computer databases and is analyzed using software specifically designed to handle large, complex data sets. Many software-as-a-service (SaaS) companies specialize in managing this type of complex data. Data analysts look at the relationship between different types of data, such as demographic data and purchase history, to determine whether a correlation exists. Such assessments may be done in-house or externally by a third-party that focuses on processing big data into digestible formats. Businesses often use the assessment of big data by such experts to turn it into actionable information.

II. CHARACTERSTICS OF BIG DATA

Big data is enormous, far surpassing the capabilities of normal data storage and processing methods. The volume of data determines if it can be categorized as big data. Large data sets are not limited to a single kind of data—instead, they consist of various kinds of data. Big data consists of different kinds of data, from tabular databases to images and audio data regardless of structure. The speed at which data is generated. In Big Data, new data is constantly generated and added to the data sets frequently. This is highly prevalent when dealing with continuously evolving data such as social media, IoT devices, and services. There will inevitably be some inconsistencies in the data sets due to the enormity and complexity of big data. Therefore, you must account for variability to properly manage and process big data. The usefulness of Big Data assets. The worthiness of the output of big data analysis can be subjective and is evaluated based on unique business objectives.

III. EXSISTING SYSTEM

An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages. To support access control for secure data sharing in the

encrypted cloud media centre, basically there are two widely popular approaches in the literature. The first kind of approach is based on attribute-based encryption (ABE) where a content provider can specify an associated access structure over attributes, and thus the cipher text stored in the cloud can only be decrypted by users whose attributes satisfy that access structure. The latter kind is based on proxy re-encryption (PRE) where the cloud acts as a proxy to help delegate the decryption rights to authorized users in a controllable manner. Compared with ABE, PRE could be more advantageous in the sense that, in ABE the content provider needs to download, decrypt, and re-encrypt data when access policies change frequently. This work focuses on PRE for secure media sharing in the encrypted cloud media centre. Digital watermarking is a kind of technique that provides viable solutions to the problem of tracing illegal content redistribution. Typically, it works by first imperceptibly embedding a unique watermark in each copy of the plain media content, and later detecting the existence of the unique watermark from a suspicious copy for traitor tracing. Earlier watermarking schemes had a limitation though: a malicious content provider could frame a user by unfairly accusing him of leaking a media object. To solve this problem, a user should be able to argue against that during a dispute. While ensuring traceability, fair watermarking further provides fairness to prevent the content provider from framing users. However, for secure cloud-based media sharing, how to properly apply fair watermarking to enable fair traitor tracing is not yet clear and remains to be fully explored.

Disadvantages

- There is no security in email data sharing
- Only analysed the activity of mail access
- Easily hack the uploaded data

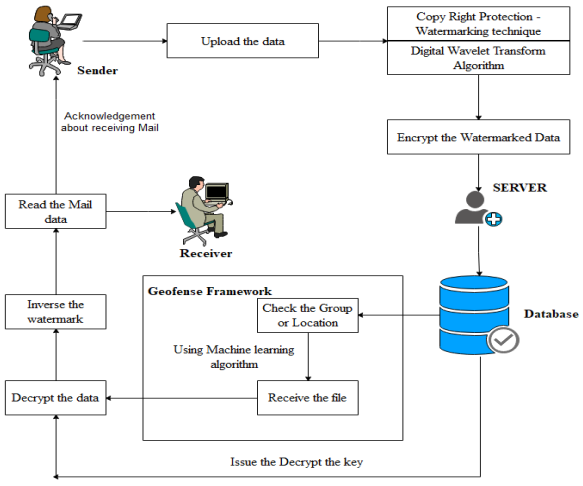
IV. PROPOSED SYSTEM

Security in Information and Communication Technology is defined as adequate protection of information against unauthorized disclosure, unauthorized modification and unauthorized withholding. It has a close relationship with privacy as insecure information cannot ensure users privacy. In E-mail messaging, security can be defined as the ability of the system to provide i) privacy, ii) sender authentication, iii) message integrity, iv) non-repudiation, and v) consistency. E-mail system consists of a number of hardware and software components that follow some defined standards. These standards also include standards for message addressing and formatting and a number of related protocols. Simple Mail Transport Protocol is the primary and the most widely adopted protocol for e-mail delivery. It lacks security features for privacy and authentication of sending party. E-mail in plain text passes from sender to recipient through many intermediaries like routers, and mail servers. It is thus, inherently vulnerable to both physical and virtual eavesdropping as malicious attackers who gain access to these intermediaries can read e-mails. Further, E-mail Service Providers (ESPs) have capabilities to store copies of e-mail messages even when these are deleted by the users. From their mailboxes. It has no mechanism to authenticate the sender or other trusted fields in any way. It does not verify or validate the senders e-mail address or other header fields. As such senders can lie about their true identities, date and time of creation of message, return address and other details which result in security challenges of different types. In this project, we can implement the framework to authenticate the users and also provide the security based on geofense framework. This framework include the watermarking, encryption and machine learning techniques. Sender can send the file and watermarked by discrete wavelet transform algorithm and also encrypted using AES algorithm. Then send the file to appropriate uses from the specific groups. And also send notification about unauthorized access.

Advantages

- It avoids the illegal distribution of shared data in storage.
- The user's watermark is well protected against the hackers.
- All the private data are well protected against the cloud and the goal of data confidentiality is achieved. The Content Provider should be endowed with the capability to trace illegal content redistribution.

V. SYSTEM DESIGN



VI. SYSTEM IMPLEMENTATION

MODULES

- Email Server Framework
- Data sharing
- Secure the data
- Group selection
- Notification with acknowledgement

After the key invokes, receiver download the data in watermarked format by using AES decryption. This file can't use by other users. Finally send the acknowledgement to sender about the status of email based on receiver.

VII. CONCLUSION

Propose a combined cryptography and watermarking techniques for secure transmission of information through E-Mail server. Discrete Wavelet technique is used for watermarking and AES cryptography is used for encryption purposes. The proposed technique is not only designed to provide copyright protection; however, it is proposed to provide integrity and authentication services for the media data based on Geofense framework. It includes the Machine learning algorithm to choose group data sharing based on location of group. Therefore, its target is not to be robust against modification attacks, but its target is to detect any illegal activities on the watermarked information. The ability of this technique is identified to check if the integrity and authentication of the shared information are corrupted at the receiver end. At the receiver side the proposed technique detected this modification and sent a message to the content provider regarding illegal distribution. And also provide mail delivery system to know about status of mail at recipient side.

VIII. ACKNOWLEDGEMENT

I express my sincere thanks to Department of Computer Science and Dhanalakshmi Srinivasan Engineering College(Autonomous), Perambalur

REFERENCES

[1] Abdelsatir, Eltigani B., and Mohammad H. Alrashdan. "On the Implementation of a Secure Email System with ID-based Encryption." 2019 International Conference on Advances in the Emerging Computing Technologies (AECT). IEEE, 2020.

[2] Nemavarkar, Apeksha, and Rajesh Kumar Chakrawarti. "A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography." 2015 International Conference on Computer, Communication and Control (IC4). IEEE, 2015.

[3] Liyanage, Geethapriya, and Shantha Fernando. "A comprehensive secure email transfer model." 2017 IEEE International Conference on Industrial and Information Systems (ICIIS). IEEE, 2017.

[4] Singh, Priyanka, et al. "S3Email: A method for securing emails from service providers." 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2017.

[5] Huo, Bo, Yihong Long, and Jinglin Wu. "A Secure Web Email System Based on IBC." 2017 13th International Conference on Computational Intelligence and Security (CIS). IEEE, 2017.

[6] Xuan, Jiaxing, 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). IEEE, 2016.

[7] Indrayani, Rini, PramuditaFerdiansyah, and Dhimas Adi Satria. "Effectiveness comparison of the AES and 3DES cryptography methods on email text messages." 2019 International Conference on Information and Communications Technology (ICOIACT). IEEE, 2019.

[8] Soualmi, Abdallah, Adel Alti, and LamriLaouamer. "A blind image watermarking method for personal medical data security." 2019 International Conference on Networking and Advanced Systems (ICNAS). IEEE, 2019.

[9] Om, Khandu. "Secure email gateway." 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM). IEEE, 2017.

[10] Wei, Jianghong, et al. "Enabling (End-to-End) Encrypted Cloud Emails With Practical Forward Secrecy." IEEE Transactions on Dependable and Secure Computing (2021).