e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

Enabling (End-To-End) Encrypted Cloud Emails with Practical Forward Secrecy

Hosanna Christy.D, Jeevitha.A, Kanimozhi.M, Kanishka.M, Guide : Mr .S.Karthick Kumar

Students, Department of CSE, Gnanamani College of Technology, Namakkal, India

AP, Department of CSE, Gnanamani College of Technology, Namakkal, 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. The problem has become more critical with the increasing use of the Internet and digital technologies. However, making the protection of copyright is more complex and difficult. Digital watermarking came up as a solution for copyright protection problem. In proposed approach implement 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. Unauthorized or illegal access can identify, when user information does not match with embedded information. This proposed application helps to track the illegal access and avoid the content re-distribution in email environment. And also provide group data sharing and also provide acknowledgement system for mail delivery system.

KEYWORDS: Data protection, Email server, Cryptography, Watermarking, Group selection

I. INTRODUCTION

Electronic mail (Email) is a method in transmitting digital messages between senders and recipients by telecommunication, namely Internet. Most email programs such as Gmail, Yahoo, Hotmail etc have make it easy in sending file attachments. The file attachments can be documents, photos, music and videos. Email can be easily accessed using digital devices such as computer,notebook, smartphone or I-pad. This has made convenient to all users like to use the Email. However, the communication or connection between senders and recipients are not confidential through the internet.

There is software that can sniff Internet packet to obtain information such as system password, private documents or for monitoring purpose. These software or tools are used by attackers on a network to obtain confidential data and attachment. Thus, the confidentiality, integrity, and authentication of that information can be abused. 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. Email authentication is a technical solution toproving that an email is not forged. In other words, it provides a way to verify that an email comes from who it claims to be from. Email authentication is most often used to block harmful or fraudulent uses of emailsuch as phishing and spam.

Email Services have been started to emerge as a result of the contrary advancements within the Internet applications technologies, as well as the novel infrastructures and platforms which are dominating today's WWW. Cloud email services have been recently introduced to the public since less than a decade. This evolution started when the first cloud based application "Send mail" was introduced. To make e-mail communication secure and private, e-mail servers incorporate one or more security features using add-on security protocols. The add-on security protocols provide a reasonable security but have several limitations. This project discusses limitations of e-mail security protocols, analyses and evaluates their effectiveness in e-mail servers. It also proposes methods to improve efficiency of e-mail servers in detecting spoofed e-mails from domains that do not follow any standard anti-spoofing protocol. Further, it

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

presents results of studies carried out to appraise e-mail user practice; knowledge of security protocols and their confidence in e-mail system. The email server system shown in fig 1.

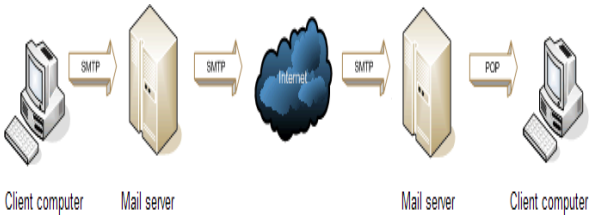

Fig 1: Email server system

II. RELATED WORK

Abdelsatir, Eltigani B, et.al,…[1] implemented securing email communications is increasingly demanded and fairly essential.Most of today's encryption schemes use techniques such as PGP and S/MIME that encrypts the entire message between the sender and the receiver. Conventional Public Key Infrastructure (PKI) systems rely on digital certificates to associate the identity of a user to a public key. The result is a digital certificate that should be effectively and constantly managed. The storage, distribution, and revocation of these certificates is a source of concern when it comes to real-world implementation. For example, X.509 PKI is the most flexible available format of PKI models. In fact, there is a wide gap between real-world business demands and traditionalX.509 model offerings as current commercial applications often need to adapt their inner workings to beable to work with X.509 certificates. Currently, many email systems are based on schemes such as S/MIME,PGP and PKI to secure communication. However, authentication methods utilized in these systems can become costly with the growing burden of certificate management and pre- enrolment as the number of users increases. In this paper, a secure email framework whiletaking into account Identity-Based Encryption without pairing is considered. The proposed system provides secure email environment that eliminates PKI hassles witheffortless key creation and management.

Nemavarkar, Apeksha, et.al,…[2] proposes the new idea of the multilevel email files security structural engineering ISA-CC through known parameters. Improved functionalities like picture validation, pressure by lossless pressure calculation and encryption utilizing AES, DES with one timecushion which can be better answer for give security and it can evade different assaults over email. It may be different calculations for securing recreating the data from the target picture yet the greater part of them continues from some measure of disappointment of emit information while remaking it. The proposed technique may be utilized to attain to all the principal objectives of cryptography by a solitary mean. IA-COTPC comprises of extremely straightforward steps with no rounds when contrasted with the standard hash and MAC calculations. It would doubtlessly have low overhead, so the target of accessibility would be attained to. Encryption is finished with the most recent secure encryption standard AES, so Confidentiality is guaranteed.

Liyanage, Geethapriya, et.al,…[3]SMTP protocol is still having security weaknesses as the studies that have been done to improve this protocol which only addresses security in Application level. The model that we proposed improves security in core SMTP. In this model we introduce authentication, authorization, confidentiality and integrity into Email system. By having these security considerations, we can improve the security in message transfer. As future works, we need to design a properrevocation policy to maintain a valid list of Email servers. By having such policy we can maintain a good valid PAD. Further, we are planning to embed public key of CCS with Email server installation software.

Singh, Priyanka et.al,…[4] used as a primary form of communication and as such, email messages might contain highly sensitive information such as social security numbers, passport credentials, credit card information, etc. It is often assumed that information sent over email is available to intended parties only, which might not always be the case. This has lead to concerns over email confidentiality. Emails are stored on infrastructure belonging to email service providers (ESPs). They are generally not readby the service providers, but there exists a potential threat from these ESPs as they can have access to users' email messages. ESPs may not be able to guarantee users privacy in all scenarios due to the possibilities of various security breaches across the network. Threats from malicious external adversaries obtaining unauthorized access to these email servers and subsequently to users' emails may cause a huge loss in privacy. With growing concern over mass surveillance,

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

privacy infringement and online attacks leading to unauthorized access and data theft, there have been various attempts to add security to email communication withvarying degrees of success.

Huo, Bo, Yihong Long, et.al,…[5] implemented The secure web email system based on IBC is barely in the marketplace. The IBC cryptography technology based on pseudo-RSA is adopted to embed IBC cryptography in the original PKI/CA system, which enables the system to communicatewith mail software that supports SMIME formats. The non-plugin technology is applicable to different types of different versions of the browser. The local agent module is proposed to communicate with the browser to achieve the security of the mail processing, with universal. The browser can send messages encrypted or signature by IBC by interacting with the local proxy module sothat the message always exists in cipher text during the transmission process and is also stored in cipher text in the mail server. The user's password stored in the database is a summary of the information processed by the SHA1, which can ensure the user's password is safe and prevent the user's password from being leaked to a certain extent.

III. BACKGROUND OF THE WORK

An email server, or simply mailserver, 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 supportaccess control for secure data sharing in the encrypted cloud media centre, basically thereare 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 associatedaccess 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 needsto 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 contentprovider 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.

IV. PROPOSED WORK

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 bedefined 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. E-mail in plain text passes from sender to recipient through many intermediaries like routers, and mailservers. 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 lieabout 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 email framework. This framework includes the watermarking, encryption techniques and OTP verification step. Sender can send the file and watermarked by discrete wavelet transform algorithm and also encrypted usingECC algorithm. Then send the file to appropriate uses from the specific groups. And also send notification about unauthorized access. The proposed work is shown in fig 2.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

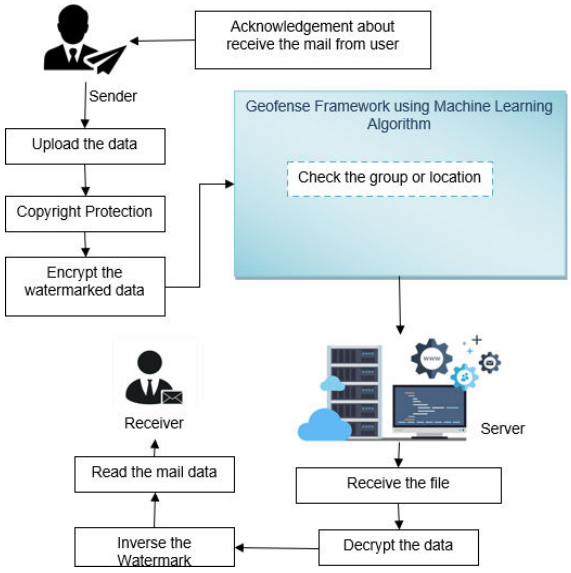

Fig 2: Proposed framework

V. DISCRETE WAVELETTRANSFORM

Discrete Wavelet transform (DWT) isa mathematical tool for hierarchical decomposition of an image. The transformation is based on decomposing asignal into wavelets or small waves, having varying frequency and limited duration. The properties of wavelet decompose an original signal into wavelet transform coefficients which contains the position information. The original signal can be reconstructed completely by performing Inverse Wavelet Transformation on these coefficients. DWT decomposes an image into sub images or sub bands, three details and one approximation. DWT has excellent spatio-frequency localization property that has been extensively utilized to identify the image areas where a disturbance can be more easily hidden. Also this technique does not require the original image for watermark detection. Digital image watermarking consists of two processes first embedding the watermark with the information and second extraction.

R′ ← WatermarkEmb(R,w, kemb1, kemb2,kemb3)

1. For each image c ∈ R

1) Divide c into s × s sized nonoverlapping blocks. Choose the low frequency blocks using DWT. The watermark is a sequence of binary bits denoted as w = w1,w2, ...,wNw. A set of blocks {BKi}Nwi=1 are chosen by a pseudorandom function as kemb1. Each block will carry one bit of the watermark.

2) For each watermark bit wi, i ∈[1, ...,Nw],

a) The pixels in block BKi are divided into two sets S0 and S1 according to a pseudorandom function with the water mark text kemb2;

b) If wi = 0, flip the bits of pixels in S0. Otherwise, flip the pixel bits in S1. In order to preserve the image quality, we make less flipping on higher bit-planes. We denote the ratios of flipped bits on 8 bit-planes as ϵ =[ϵ1, ϵ2, ..., ϵ8]. That is to say, for the i-th bit-plane, there are Nw × s2 × ϵi/2 bits willbe flipped randomly. The flipped positions are determined by kemb3 using Inverse DWT. Flip the water mark text color intoimage color.

2. Output the watermarked image set R′.

wt ← WatermarkExtra(mt,mo, kemb1, kemb2, kemb3)

1. Divide mt into nonoverlapping blocks withthe size s × s using DWT.

2. Locate the set of blocks {BKi}Nw i=1 thatcarries the watermark

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

bits w = w1,w2, ...,wNw according to thesecret key kemb1.

3. For each i ∈[1,Nw],

1) Divide the pixels in BKi into two sets S0 and S1 according to locations kemb2;

2) Flip the pixels in S0 and S1 respectively according to [∈i]8 i=1 and kemb3 to get two blocks BK0i and BK1i. Construct the corresponding block BKi from the original image with the secret key kemb1. Calculate δ0 =Σpj∈BKi;p0j∈BK0i (p0j pj)2 and δ1 = Σpj∈BKi;p1j∈BK1i (p1j− pj)2. If δ0 < δ1, the watermark bit is extracted as '0'. Else, the watermark bit is extracted as '1'.

VI. ELLPTICAL CURVECRYPTOGRAPHY

The Elliptic Curve Cryptography (ECC) algorithm is a widely used public key cryptography algorithm that is used for secure communication over the internet. The basic steps involved in the ECC algorithmare as follows:

Key Generation: The first step is to generatea pair of keys, one public and one private.The private key is kept secret by the owner, while the public key is shared with other users who wish to communicate securely.

Elliptic Curve Selection: The next step is to select an elliptic curve, which is a mathematical curve defined by an equation. The curve must satisfy certain properties to be suitable for use in the ECC algorithm,such as being non-singular and having a largeprime order.

Point Selection: A point on the elliptic curve is then selected as the base point. This point must also satisfy certain properties, such as having a large prime order and being in a subgroup of the curve.

Key Exchange: To exchange keys, the two parties each generate a random number, which is then used to calculate a shared secret. The shared secret is then used as a keyfor symmetric encryption, which is used to encrypt and decrypt messages between the parties.

Encryption and Decryption: To encrypt a message, the sender first generates a random number, which is used to calculate a point onthe elliptic curve. This point is then combined with the recipient's public key to generate a shared secret. The message is thenencrypted using a symmetric encryption algorithm and the shared secret as the key. To decrypt the message, the recipient uses their private key to generate the shared secret and then uses the same symmetric encryption algorithm to decrypt the message.

Overall, the ECC algorithm provides a secureand efficient method for key exchange and message encryption, making it a popular choice for secure communication over the internet.

V. MACHINE LEARNINGALGORITHM

In a decision tree, for predicting the class of the given dataset, the algorithm startsfrom the root node of the tree. This algorithm compares the values of root attribute with the record (real dataset) attribute and, based on the comparison, follows the branch and jumps to the next node.For the next node, the algorithm again compares the attribute value with the other sub-nodes and move further. Itcontinues the process until it reaches the leaf node of the tree. The complete process can bebetter understood using the below algorithm:

Step-1: Begin the tree with the root node,says S, which contains the complete dataset.

Step-2: Find the best attribute in the dataset using **Attribute Selection Measure (ASM).**

Step-3: Divide the S into subsets that contains possible values for the bestattributes.

Step-4: Generate the decision tree node,which contains the best attribute.

Step-5: Recursively make new decision trees using the subsets of the dataset created in step -3. Continue this process until a stage is reached where you cannot further classify thenodes and called the final node as a leaf node

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

VI. EXPERIMENTAL RESULTS

The proposed framework is implemented using ASP.NET for design and shows theresults in following figures

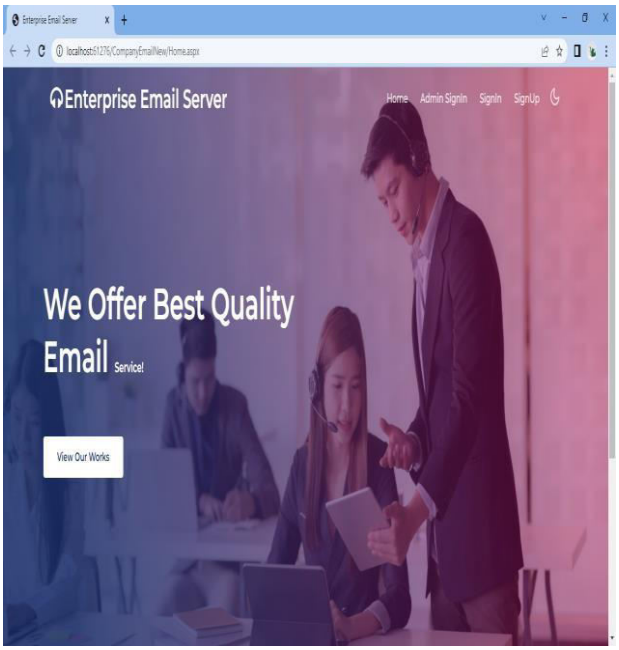

Fig 3: HOME PAGE

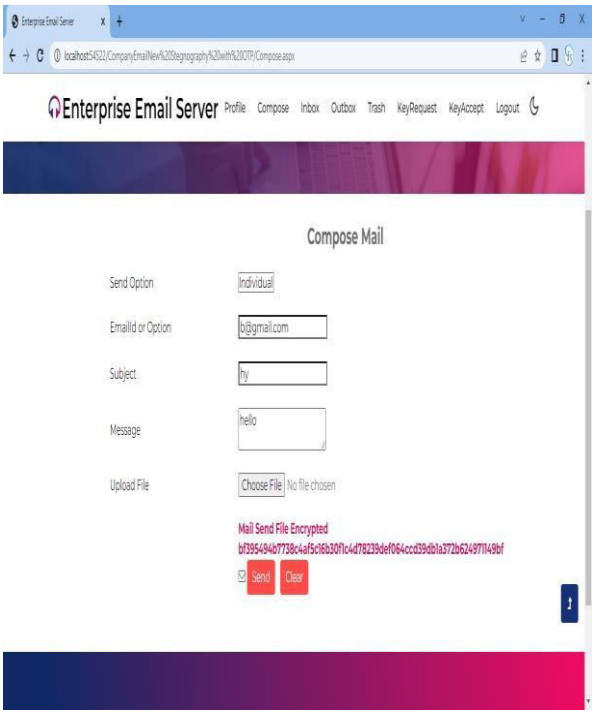

FIG 4: SECURE DATA SHARING

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

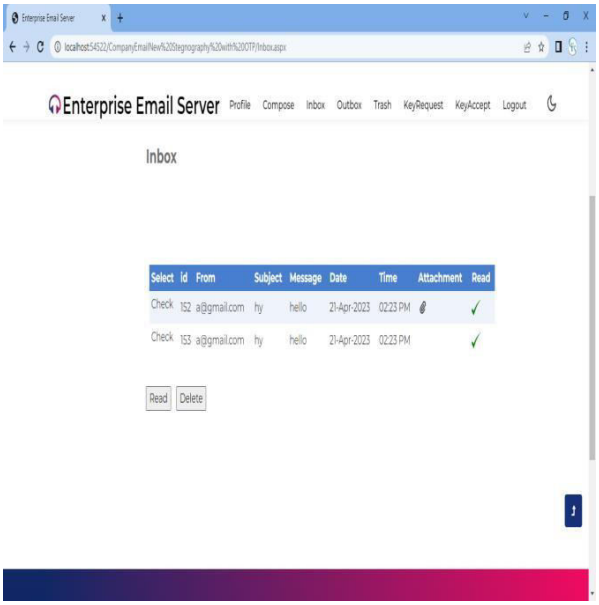

FIG 5: NOTIFICATION SYSTEM

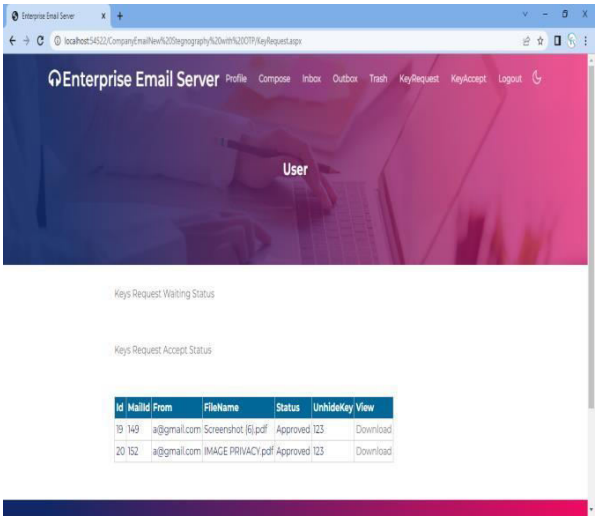

FIG 6: DOWNLOAD THE DATA

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 ECC 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 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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 5, May 2023 |

REFERENCES

1. Abdelsatir, Eltigani B., and Mohammad H. Alrashdan. "On the Implementation of a Secure Email System with ID-based Encryption." 2019 International Conference
2. on Advances in the Emerging ComputingTechnologies (AECT). IEEE, 2020.
3. Nemavarkar, Apeksha, and Rajesh KumarChakrawarti. "A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography." 2015 International Conference on Computer, Communication and Control (IC4). IEEE, 2015.
4. Liyanage, Geethapriya, and Shantha Fernando. "A comprehensive secure email transfer model." 2017 IEEE International Conference on Industrial and Information Systems (ICIIS). IEEE, 2017.
5. 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.
6. 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.
7. Xuan, Jiaxing, et al. "Design of secure and independent controllable email systembased on Identity-BasedCryptography." 2016 2nd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2016.
8. Indrayani, Rini, Pramudita Ferdiansyah, and Dhimas Adi Satria. "Effectiveness comparison of the AES and 3DES cryptography methods on email text messages." 2019 International Conference on Information and CommunicationsTechnology (ICOIACT). IEEE, 2019.
9. Soualmi, Abdallah, Adel Alti, and Lamri Laouamer. "A blind image watermarking method for personal medical data security." 2019 International Conference onNetworking and Advanced Systems(ICNAS). IEEE, 2019.
10. Om, Khandu. "Secure email gateway." 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM). IEEE, 2017.
11. Wei, Jianghong, et al. "Enabling (End- to-End) Encrypted Cloud Emails With Practical Forward Secrecy." IEEETransactions on Dependable and Secure Computing (2021).
12. Purevjav, Saranzaya, TaeYang Kim, andHoonJae Lee. "Email encryption using hybrid cryptosystem based on Android." 2016 18th International Conference on Advanced Communication Technology (ICACT). IEEE, 2016.
13. Muslim, M. A., et al. "Analysis of image watermarking with a discrete wavelet transform for digital data security." Journal of Physics: Conference Series. Vol. 1918. No.
14. IOP Publishing, 2021.
15. Kumar, Kapil, and Vikram Singh."Reverse Watermarking Technique toEnhance Cloud Data Security." (2019).
16. Barapatre, Minal, and C. N. Deshmukh. "Design & Development of Network Geo- Fencing Model for User Monitoring and it's Alertness in a Security Applications" 2019
17. Abbas, A. H., et al. "GPS based location monitoring system with geo-fencing capabilities." AIP Conference Proceedings.Vol. 2173. No. 1. AIP Publishing LLC, 2019.
18. Al-Asady, Heba Abdul-Jaleel, Osama Qasim Jumah Al-Thahab, and Saad S. Hreshee. "Robust encryption system based watermarking theory by using chaotic algorithms: A reviewer paper." Journal of Physics: Conference Series. Vol. 1818. No. 1.IOP Publishing, 2021.
19. Gautam, Aakanksha, and Vipin Vats. "Digital Data Security using Audio Watermarking & Cryptography Concepts" 2019
20. Xiao, Yan, and Guangyong Gao. "Digital watermark-based independent individual certification scheme in WSNs." IEEE Access 7(2019): 145516-145523.
21. Bagdasaryan, Eugene, 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.
22. Rodriguez Garzon, Sandro, 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.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com