



Email Security

Kadam Akanksha^{1*}, Zodage Utkarsha², Kashid Sneha³, Chavan Sanika⁴, Dr. Kazi K. S.⁵

^{1*,2,3}Student, CSE Department, SSWCOE, Solapur (MS), India

⁴Student, IT Department, SSWCOE, Solapur (MS), India

⁵Associate Professor, Department of AIDS/IT, SSWCOE, Solapur (MS), India

Email: ²zodageutkarsha24@gmail.com, ³kashidsneha9@gmail.com,

⁴sanikachavan9096@gmail.com, ⁵drkkazi@gmail.com

Corresponding Email: ^{1*}kadamakanksha50@gmail.com

Received: 25 July 2022

Accepted: 21 September 2022

Published: 18 October 2022

Abstract: A crucial network application is the email client. It is significant when it is used by the business, health, and educational groups to communicate vital information like business data, patient medical records, and so on. Data and messages can be easily transmitted between senders and receivers across internal networks or the Internet, enabling messages to be received, forwarded, saved, and broadcast to recipients. Due to its numerous features, email has become a popular choice for official communications in many companies. Electronic mail is accessible through a wide range of suitable software clients, as well as through a web browser, and is also widely used for personal usage. For the information security research community, email security becomes a critical concern. to increase the security of email.

Keywords: Image security, Mail Security

1. INTRODUCTION

Email security becomes a crucial issue for the research community in the field of information security. to strengthen email security. According to the most recent security requirements of the existing upgrades, a number of solutions and standards have been developed to maintain the trustworthiness and vitality of data interchange via e-mail. In this study, some email security methods will be suggested. We introduce each one and assess it in terms of security. various approaches and methods employed to address and improve the security of email systems There are numerous methods. Email security refers to safeguarding confidential information in email correspondence as well as account security from theft, loss, or compromise. employing misleading communications to persuade recipients to give sensitive information, download attachments, or click on links that lead to malware installation on the victim's device In an enterprise network, email is a common way for malware, spam, and phishing attempts to proliferate and compromise sensitive company data. Attackers who want



to take control of both personal and commercial email accounts frequently enter through email, so businesses should take a number of steps to strengthen email security. Security For Emails Is Important Malware can be spread through email communications and is highly harmful. via hyperlinks pointing to malicious websites or in attachments disguised to look like legitimate documents Employees frequently get phishing emails that contain malware.

2. LITERATURE REVIEW:

2.1 Security point of view:

The algorithm of encoding approach was utilised in the ref[10] research to secure the image documents. However, even if it had actually worked, from a security perspective, this encryption scheme would have been exceedingly unreliable for two reasons. First off, there isn't a hidden key. As a result, it is an encoding system rather than a genuine encryption one.

2.2 Block-Based Algorithm

The following are some of the techniques that are used: Large images cannot use the blowfish algorithm since it performs best for the lowest image block size. Higher correlation and lower entropy were the outcomes. They then suggested a new algorithm.

2.3 Steganography:

The practise of concealing sensitive information within a carrier, such as an audio, video, or image file. Since the secret information was encoded in an image file that was sent to the recipient instead of the secret information itself, this technology allowed for invisible communication. Information is being protected by the cipher text by being converted into an unintelligible form.

2.4 Particle swarm optimization (PSO):

They talked about using Particle Swarm Optimization (PSO) to tamper-proof and authenticate images. for reasons including durability, security, and accurate localisation of tampering The issues are addressed by this plan. PSO was used to extract the features in the domain of the Daubechies4 wavelet transform in order to produce the picture hash.

2.5 Virtual Private Network (VPN):

Additional data protection is offered in various application sectors, such as finance, banking, and reservation systems, by the use of virtual private network (VPN), data encryption, and data embedding techniques. In order to overcome this deficiency, the picture archiving and communications system (PACS), an integrated management system for preserving and transmitting medical image data, was created.

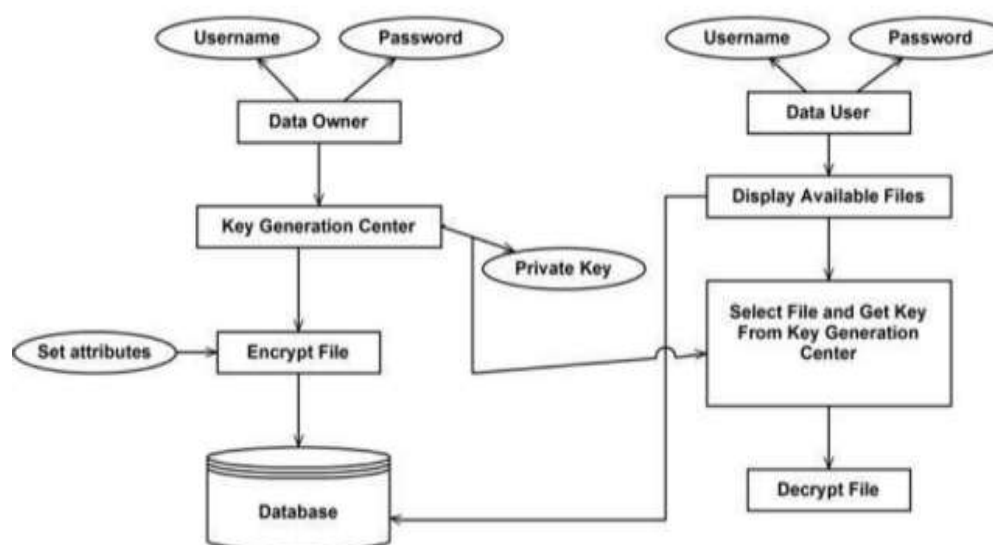
2.6 Summery:

The privacy of cloud-based data is attained through the use of encryption methods. To accomplish data cryptographic security, a variety of strategies and methods are used in network security. The most popular technique today is attribute-based encryption (ABE). If a user submits an access request to the cloud, the cloud will provide cypher text data to that user, who must use your private key to decrypt the data.

3. METHODOLOGY

The block diagram functions as follows.

1. Data owner chooses which photographs to upload after entering their username and password.
2. A special key will be generated at the key generation centre to encrypt this image.
3. The photos will be keyed into a database for storage. User will select image and request for the key to owner. After that user will enter the key and the image will get decrypt to the original form.



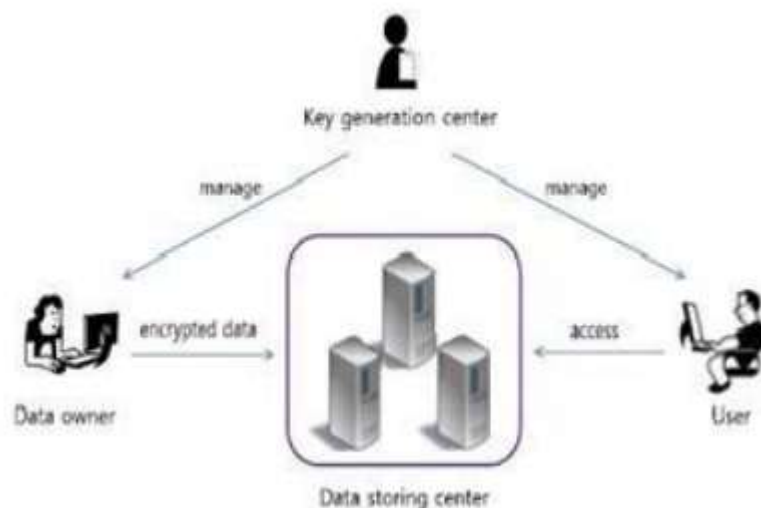
A. Registration Phase: Initially, the user enters their username, password, and mobile number. They are then given the option to select the photo matrix after selecting the security level. The amount of messages relies on that number when the security level is set to $2n$. After entering their communications in the message box, the user must choose how they should be converted before having the converted communications shown as QR pictures in the registration part below.

B. Login Phase: Depending on the security level matrix of the presented QR pictures, the user enters their user ID and password during the login phase. The user registers the appropriate encoded image during the registration process.

C. Confirmation Phase: The system examines the level-by-level selection of the image, or compares the data entered with the data entered at registration time; if any level is unsuccessful, the system may immediately and without warning terminate the user's

session. The user will receive the OTP on their registered mobile device if everything is correct.

- D. Key generation centre:** the principal organisation in charge of creating private and public CP-ABEs. For users, it has the power to give, cancel, and alter attribute keys. On the basis of each user's unique characteristics, it provides them various access permissions. It is thought to be serious but intriguing.
- E. Data-storing centre:** It is a business that provides a service for data exchange. Its duties include providing pertinent content offerings and controlling access to the data storage for outside users.
- F. Data owner:** It is a client who want to upload data onto the external data centre in order to facilitate cost savings or simpler sharing. A data owner is in charge of creating a (attribute-based) access policy and enforcing it on its own data by encrypting the data covered by the policy before distributing it.
- G. User:** The organisation that needs access to the data is that organisation. A user will be able to decrypt the cypher text and acquire the data if they have a set of characteristics that satisfy the access policy for the encrypted data and are not revoked in any of the valid attribute groups.



4. RESULT



Fig1. Auto Generated unique QR code as password

The system generates a unique QR code using the QR Encryption technique that is used to register users.

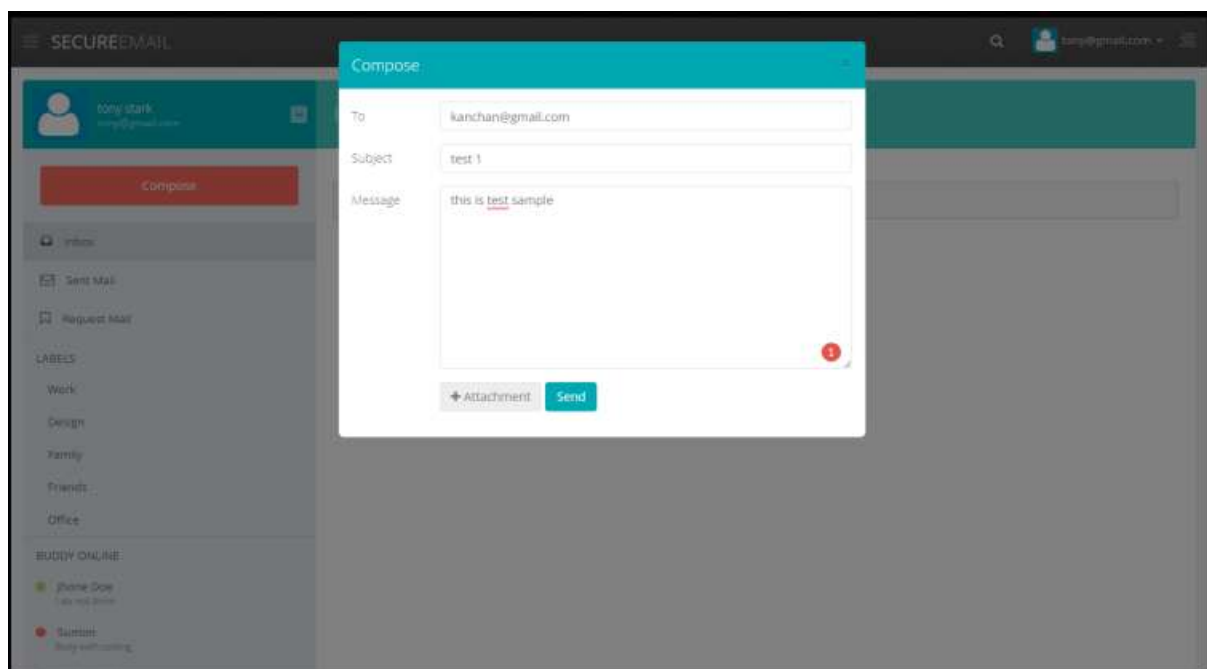


Fig2. User Mail Compose Form

The data owner (first user) can compose his mail for the receiver (second user) with image file as a attachment

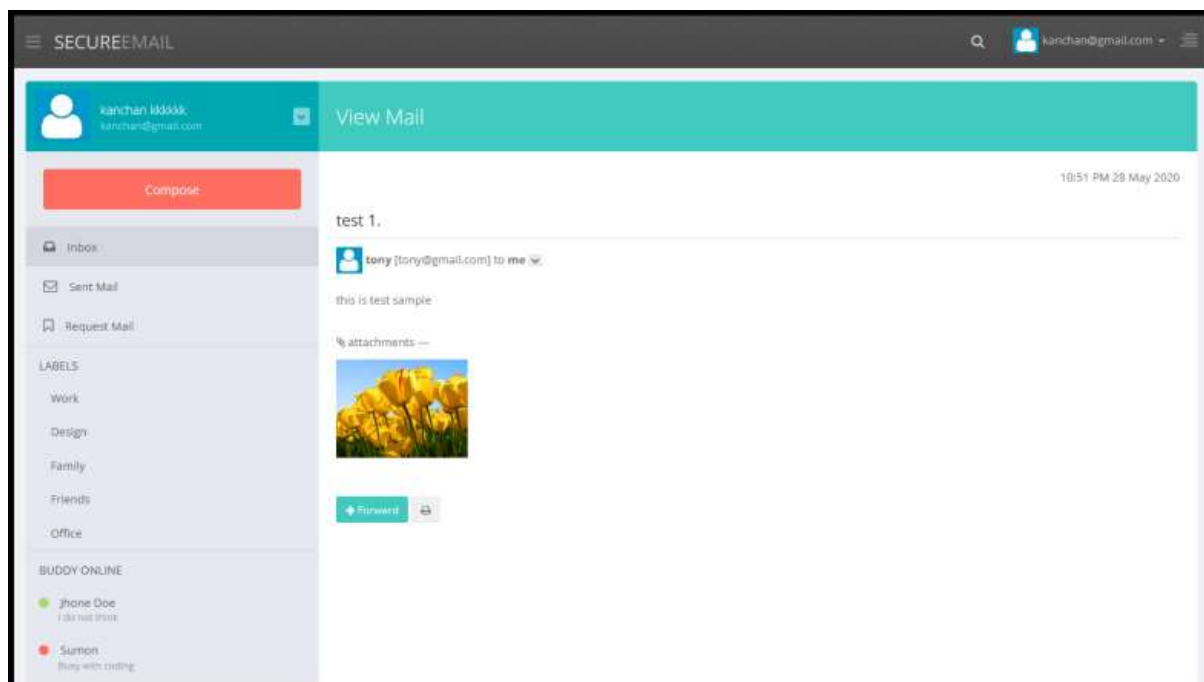


Fig. The receiver (Second user) receives Mail to his inbox

The receiver (second user) receives his mail sent by the data owner (first user) with image file as a attachment.

5. CONCLUSION

The proposed system overcomes the drawbacks found in the present existing mail servers regarding security by providing better security for the mails especially containing critical information. Hacking has become one of the greatest threats faced in today's mailing systems due to the usage of only one level of security, i.e., a login-password system. The developed application with 3 layer authentication provides enhanced security for the critical mails shared via Internet and ensures that the users don't have to worry about the message being hacked. It builds a secure system that will ensure that the critical information is not leaked or misused thus making it an ideal mailing system. It adds privacy, authentication, message integrity, and nonrepudiation to plaintext email.

6. REFERENCE

1. J.-M. Zhu and J.-F. Ma, "Improving Security and Efficiency in Attribute Based Data Sharing," IEEE Transactions on knowledge and data engineering , vol. 25, no. 10, october 2013
2. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.
3. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.



4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
5. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. Int'l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009.
6. M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority AttributeBased Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
7. S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09), pp. 256-276, 2009.
- a. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.
8. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," Proc. Int'l Colloquium Automata, Languages and Programming (ICALP), pp. 579- 591, 2008.
9. Gonzalo Alvarez, Shujun Li, Luis Hernandez "Analysis of security problems in a medical image encryption system"
10. Mohammad Ali Bani Younes and Arnan Jantan "Image Encryption Using Block-Based Transformation Algorithm "
11. Pritam Kumari, Chetna Kumar, Preyanshi, Jaya Bhushan "Data Security Using Image Steganography And Weighing Its Techniques"
12. K. Kuppusamy and K. Thamodaran "PSO based optimized security scheme for image authentication and tamper proofing "
13. Miss. Kamble Sunayana Nivrutti, Prof. Gund V. D., et al, "Multimodal Biometrics Authentication System Using Fusion Of Fingerprint And Iris", International Journal of Trends in Scientific research and Development (IJTSRD), Sep-Oct 2018, Vol 2, Issue 6, pp 1282-1286
14. Kazi K. S., "Significance And Usage Of Face Recognition System", Scholarly Journal For Humanity Science And English Language, Feb-March 2017, Vol 4, Issue 20, pp 4764-4772.
15. Prof. Kazi K. S., "Situation invariant Face Recognition using PCA and Feed forward Neural Networks", Proceeding of ICAEST, Feb 2016, ISBN: 978 - 81 - 930654 - 5 - 4, pp 260-263.
16. Prof. Nagarkar Raviraj Prakash, et al., "Pose invariant Face Recognition using Neural Networks and PCA", International Engineering Journal For Research & Development, Vol 4 special issue, pp 1-4.<https://doi.org/10.17605/OSF.IO/CEVUG>
17. Miss. A. J. Dixit, et al, "Iris Recognition by Daugman's Method", International Journal of Latest Technology in Engineering, Management & Applied Science, July 2015, Vol 4, Issue 6, pp 90-93.
18. Wale Anjali D., Rokade Dipali, et al, "Smart Agriculture System using IoT", International Journal of Innovative Research In Technology, 2019, Vol 5, Issue 10, pp.493-497.
19. Ms. Machha Babitha, C Sushma, et al, "Trends of Artificial Intelligence for online exams in education", International journal of Early Childhood special Education, 2022, Vol 14, Issue 01, pp. 2457-2463.



20. Pankaj R Hotkar, Vishal Kulkarni, et al, "Implementation of Low Power and area efficient carry select Adder", International Journal of Research in Engineering, Science and Management, 2019, Vol 2, Issue 4, pp. 183-184.
21. Karale Nikita, Jadhav Supriya, et al, "Design of Vehicle system using CAN Protocol", International Journal of Research in Applied science and Engineering Technology, 2020, Vol 8, issue V, pp. 1978-1983, <http://doi.org/10.22214/ijraset.2020.5321>.
22. Dr. J. Sirisha Devi, Mr. B. Sreedhar, et al, "A path towards child-centric Artificial Intelligence based Education", International journal of Early Childhood special Education, 2022, Vol 14, Issue 03, pp. 9915-9922.
23. Kutubuddin Kazi, "Lassar Methodology for Network Intrusion Detection", Scholarly Research Journal for Humanity science and English Language, 2017, Vol 4, Issue 24, pp.6853-6861.
24. Mr. D. Sreenivasulu, Dr. J. Sirishadevi, et al, "Implementation of Latest machine learning approaches for students Grade Prediction", International journal of Early Childhood special Education, June 2022, Vol 14, Issue 03, pp. 9887-9894.
25. Kazi Kutubuddin Sayyad Liyakat, Nilima S. Warhade, Rahul S. Pol, Hemlata M. Jadhav, Altaf O. Mulani, "Yarn Quality detection for Textile Industries using Image Processing", Journal Of Algebraic Statistics, July 2022, Vol 13, Issue 3, pp. 3465-3472.
26. Prof. Kazi K.S., Miss Argonda U A, "Review paper for design and simulation of a Patch antenna by using HFSS", International Journal of Trends in Scientific Research and Development, Jan-Feb 2018, Vol 2, issue-2, pp. 158- 160.
27. Ms. Yogita Shirdale, et al, "Analysis and design of Capacitive coupled wideband Microstrip antenna in C and X band: A Survey", Journal GSD-International society for green, Sustainable Engineering and Management, Nov 2014, Vol 1, issue 15, pp. 1-7.
28. Prof. Kazi Kutubuddin Sayyad Liyakat, "Situation Invariant face recognition using PCA and Feed Forward Neural network", Proceeding of International Conference on Advances in Engineering, Science and Technology, 2016, pp. 260- 263.
29. Prof. Kazi Kutubuddin Sayyad Liyakat, "An Approach on Yarn Quality Detection for Textile Industries using Image Processing", Proceeding of International Conference on Advances in Engineering, Science and Technology, 2016, pp. 325-330.
30. Ms. Shweta Nagare, et al., "Different Segmentation Techniques for brain tumor detection: A Survey", MM- International society for green, Sustainable Engineering and Management, Nov 2014, Vol 1, issue 14, pp.29-35.
31. Miss. A. J. Dixit, et al, "A Review paper on Iris Recognition", Journal GSD International society for green, Sustainable Engineering and Management, Nov 2014, Vol 1, issue 14, pp. 71-81.
32. Prof. Suryawanshi Rupali V, et al, "Situation Invariant face recognition using Neural Network", International Journal of Trends in Scientific research and Development (IJTSRD), May-June 2018, Vol 2, issue-4, pp. 995-998.
33. Ms. Shweta Nagare, et al., "An Efficient Algorithm brain tumor detection based on Segmentation and Thresholding ", Journal of Management in Manufacturing and services, Sept 2015, Vol 2, issue 17, pp.19-27.
34. Miss. A. J. Dixit, et al, "Iris Recognition by Daugman's Algorithm – an Efficient Approach", Journal of applied Research and Social Sciences, July 2015, Vol 2, issue 14, pp. 1-4.



35. Kazi K. S., Shirgan S S, “Face Recognition based on Principal Component Analysis and Feed Forward Neural Network”, National Conference on Emerging trends in Engineering, Technology, Architecture, Dec 2010, pp. 250-253.
36. Ms. Yogita Shirdale, et al., “Coplanar capacitive coupled probe fed micro strip antenna for C and X band”, International Journal of Advanced Research in Computer and Communication Engineering, 2016, Vol 5, Issue 4, pp. 661-663.
37. Rahul S. Pole, Amar Deshmukh, MakarandJadhav, et al, “ iButton Based Physical access Authorization and security system”, Journal of Algebraic Statistics, 2022, Vol 13, issue 3, pp. 3822-3829.
38. Dr. Kazi Kutubuddin, V A Mane, Dr K P Pardeshi, Dr. D.B Kadam, Dr. Pandiyaji K K, “Development of Pose invariant Face Recognition method based on PCA and Artificial Neural Network”, Journal of Algebraic Statistics, 2022, Vol 13, issue 3, pp. 3676-3684.
39. Ravi Aavula, Amar Deshmukh, V A Mane, et al, “Design and Implementation of sensor and IoT based Remembrance system for closed one”, Telematique, 2022, Vol 21, Issue 1, pp. 2769- 2778.
40. Kutubuddin Kazi, “Systematic Survey on Alzheimer's (AD) Diseases Detection”, 2022, DOI: 10.13140/RG.2.2.22369.58722
41. Kutubuddin Kazi, “A Review Paper Alzheimer”, 2022, DOI: 10.13140/RG.2.2.11464.39684
42. Kutubuddin Kazi, “Multiple Object Detection And Classification Using Sparsity Regularized Pruning On Low Quality Image/Video With Kalman Filter Methodology(Literature Review)” 2022, DOI: 10.13140/RG.2.2.19853.00488
43. Kutubuddin Kazi, “Implementing YOLO”, 2022, DOI: 10.13140/RG.2.2.13142.11841
44. Kutubuddin Kazi, “Multiple Object Detection And Classification Using Sparsity Regularized Pruning On Low Quality Image/Video With Kalman Filter Methodology (Working)” 2022, DOI: 10.13140/RG.2.2.16497.56161
45. Kutubuddin Kazi, “Multiple Object Detection And Classification Using Sparsity Regularized Pruning On Low Quality Image/Video With Kalman Filter Methodology(Different Techniques)” ,2022, DOI: 10.13140/RG.2.2.29919.33442
46. Kutubuddin Kazi, “Multiple Object Detection And Classification Using Sparsity Regularized Pruning On Low Quality Image/Video With Kalman Filter (Hardware and software requirements)” 2022, DOI: 10.13140/RG.2.2.36630.22086
47. M. Sunil Kumar, D. Ganesh et al, “Deep Convolution Neural Network based solution for detecting plan diseases”, International Journal of Pharmaceutical Negative Results, 2022, Vol 13, Issue- Special Issue 1, pp. 464-471
48. Dr. Kazi Kutubuddin et al , “Development of Machine Learning based Epileptic Seizureprediction using Web of Things (WoT)” , NeuroQuantology, 2022, Vol 20, Issue 8, pp. 9394- 9409
49. Dr. K. P. Pardeshi et al, “Implementation of Fault Detection Framework For Healthcare Monitoring System Using IoT, Sensors In Wireless Environment”, TELEMATIQUE, 2022, Vol 21, Issue 1, pp. 5451 - 5460
50. Dr. B. D. Kadam et al, “Implementation of Carry Select Adder (CSLA) for Area, Delay and Power Minimization”, TELEMATIQUE, 2022, Vol 21, Issue 1, pp. 5461 – 5474