International Journal of Engineering & Extended Technologies Research (IJEETR)

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802444

Smart Grid Monitoring using IoT with Renewable Integration

Dr.S.Saravanan, Mr.G.Dinesh Kumar, Ajith S, Kaviyarasan S, Lokikrishna S D, Gowtham R

Department of Electrical and Electronics Engineering, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: A new blind authentication method based on the secret sharing technique with a data repair capability for color document images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a color document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original color image to form a PNG image. During the embedding process, the computed share values are mapped into a range of alpha channel values near their maximum value of 255 to yield a transparent stego-image with a disguise effect. In the process of image authentication, an image block is marked as tampered if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane. Data repairing is then applied to each tampered block by a reverse Shamir scheme after collecting two shares from unmarked blocks. Measures for protecting the security of the data hidden in the alpha channel are also proposed.

KEYWORDS: Data hiding, data repair, grayscale document image, image authentication, Portable Network Graphics (PNG)image, secret sharing.

I. INTRODUCTION

Digital image is a form for preserving important information. However, with the fast advance of digital technologies, it is easy to make visually imperceptible modifications to the contents of digital images. How to ensure the integrity and the authenticity of a digital image is thus a challenge. It is desirable to design effective methods to solve this kind of imageauthentication problem, particularly for images of documents whose security must be protected. It is also hoped that, if part of a document image is verified to have been illicitly altered, the destroyed content can be repaired. Such image content authentication and self-repair capabilities are useful for the security protection of digital documents in many fields, such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on.

Document images, which include texts, tables, line arts, etc., as main contents, are often digitized into gray scale images with two major gray values, one being of the background (including mainly blank spaces) and the other of the foreground (including mainly texts). It is noted that such images, although gray valued in nature, look like binary. The binary-like gray scale document images may be threshold into binary ones for later processing, but such a thresholding operation often destroys the smoothness of the boundaries of text characters, resulting in visually unpleasant stroke appearances with zigzag contours. Therefore, in practical applications, text documents are often digitized and kept as grayscale images for later visual inspection.

The image authentication crisis is difficult for a binary document image because of its simple binary nature which leads to perceptible changes after authentication signals are embedded in the image pixels. Such changes will arouse possible doubts from attackers. A good solution to such binary image authentication thus should take into account not only the security issue of preventing image tampering, but also the necessity of keeping the visual quality of the resulting image. Several methods for binary image authentication have been proposed in the past.C. S. Lu and H. Y. M. Liao[2] proposed a multipurpose watermarking scheme which can simultaneously achieve copyright protection and content authentication by hiding multipurpose watermarks at the same time.Wu and Liu [4] manipulated the so-called flippable pixels to create specific relationships to embed data for authentication and annotation of binary images. H. Y. Kim and A.[7] proposed a set of pseudorandom pixels in a binary or halftone image are chosen and cleared, and authentication

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

codes are accordingly computed and inserted into selected random pixels.Yang and Kot [5] proposed a two-layer binary image authentication method in which one layer is used for checking the image fidelity and the other for checking image integrity. In the method, a connectivity-preserving transition criterion for determining the flippability of a pixel is used for embedding the cryptographic signature and the block identifier.Yang and Kot [6] proposed a pattern-based data hiding method for binary image authentication in which three transition criteria are used to determine the flippabilities of pixels in each block, and the watermark is adaptively embedded into embeddable blocks to deal with the uneven embed ability condition in the host image.Lee et al. [8] proposed a Hamming-code-based data embedding method that flips one pixel in each binary image block for embedding a watermark,yielding small distortions and low false negative rates. Here,an authentication method is proposed which deals with binary-like grayscaledocument images as a replacement for of pure binary ones, and solves concurrently the problems of image tampering detection and visual quality keeping. In this study, a method for authentication of document images with a supplementary self-repair capability for fixing tampered image data is proposed. The input cover image is assumed to be a binary-like grayscale image with 2 major gray values. After the proposed method is applied, the cover image is transformed into a stego-image in the PNG format with an supplementary alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be verified by the proposed technique for its authenticity. Integrity modifications of the stegoimage can be detected by the method at the block level and repaired at the pixel level.

In case that the alpha channel is totally removed from the stego-image, the intact resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The proposed method is based on the so-called (k,n)-threshold secret sharing scheme proposed by Shamir in which a secret message is transformed into n shares for keeping by n participants; and when k of the nshares, not necessarily all of them, are collected, the secret message can be recovered without any loss. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

II. PROPOSED SYTEM

The secured color document transfer using PNG image with data repair capability using alpha channel is the proposed system.

THE SHAMIR METHOD FOR SECRET SHARING

The proposed approach to secret image sharing is based on the (k,n)-threshold secret sharing method proposed.In this section we describe how to use the Shamir method for conventional secret sharing. By the Shamir method, to generate n shares for a group of nsecret sharing participants from a secret integer value y for the threshold k, we can use the following (k-1)-degree polynomial in the following way.

Algorithm 1: (k,n)-threshold secret sharing

Input: Secret d in the form of an integer, number of participants, and threshold.

Output : Shares in the form of integers for the participants to keep.

Step 1 :Choose randomly a prime number that is larger than d.

Step 2: Select k-1 integer values within the range of 0 through p-1.

Step 3 : Select n distinct real values $x_1, x_2, \ldots, x_n$.

Step 4 : Use the following (k-1)-degree polynomial to compute n function values,

$F(x_i)$ called partial shares for i=1,2,……,n, i.e.,

$$F(x_i) = (d + C_1 x_i + C_2 x_i^2 + \cdots + C_{k-1} x_i^{k-1})_{\text{mod } p} \qquad (1)$$

Step 5 : Deliver the 2-tuple $(x_i, F(x_i))$ as a share to the i th participant where i=1,2,……,n.

The k coefficients, namely d and c_k through c_{k-1}in Eqn. (1) above, it is necessary together at least shares from the n participants to form k equations of the form of Eqn.(1) to solve these k coefficients in order to recover secret d. This explains the term threshold for k and the name (k,n) -threshold for the Shamir method . Below is a description of the just-mentioned equation-solving process for secret recovery.

Algorithm 2: Secret recovery

Input :k shares collected from the n participants and the prime number p with both k and p being those used in Algorithm 1.

Output :Secret d hidden in the shares and coefficients ci used in Eqn. (1) in Algorithm 1, where i=1, 2 k-1.

Step1 : Use the k shares $(x_1, F(x_1))$, $(x_2, F(x_2))\ldots (x_k, F(x_k))$ to setup

$$F(x_j) = (d + C_1 x_j + C_2 x_j^2 + \cdots + C_{k-1} x_j^{k-1})_{\text{mod } p} \quad (2) \qquad \text{Where } j=1,2\ldots k.$$

International Journal of Engineering & Extended Technologies Research (IJEETR)

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

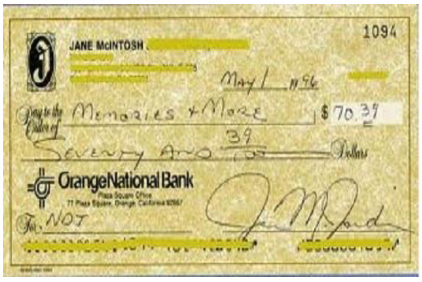
Step2: Solve the k equations above by Lagrange's interpolation to obtain d as Follows

$$d=(-1)^{k-1}[F(x_1)\frac{x_2x_3\ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)}+ F(x_2)\frac{x_1x_3\ldots x_k}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)}+\cdots+ F(x_k)\frac{x_1x_2\ldots x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}]\bmod p$$

Step 3: Compute $c_1$through $c_{k-1}$by expanding the following equality and comparing the result with Eqn. (2) in Step 1 while regarding variable x in the equalitybelow to be xj in (2):

$$F(x)=[F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_k)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)}+F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_k)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)}+\cdots + F(x_k)\frac{(x-x_1)(x-x_2)\ldots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}]\bmod p$$

In the above algorithm Step3 is in addition included for the purpose of computing the values of parameters $c_i$in the proposed method. In other applications, if only the secret value need be recovered, this step may be eliminated.If fewer than k secret shares are collected, the k unknowns cannot be solved and the desired y value cannot be reconstructed.



Color Image

Input Image

PNG Image

Fig 1:convertion of color image to PNG image

International Journal of Engineering & Extended Technologies Research (IJEETR)

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

IMAGE AUTHENTICATION AND DATA REPAIRING

PNG image from a binary-type grayscale document image S with an alpha channel plane is created . The actual image S may be assumed as a grayscale channel plane of the PNG image. Then, S is converted to binary form with moment-preserving threshold, yielding a binary version of S, which we denote as S. Data image for authentication and repairing are then computed from Sb and taken as an input to Shamir's secret sharing scheme, to generate n secret shares of the data. The share values are mapped subsequently into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Lastly, the mapped secret shares are randomly entrenched into the alpha channel for the function of promoting the security, protection and data repair capability.

The alpha channel plane is used for carrying data for authentication and repairing, so no demolition will occur to the input image in the process of verification. On the contrary, traditional image authentication methods often sacrifice part of image contents, such as LSB's or pixels that can be flipped, to provide accommodation to data used for authentication.

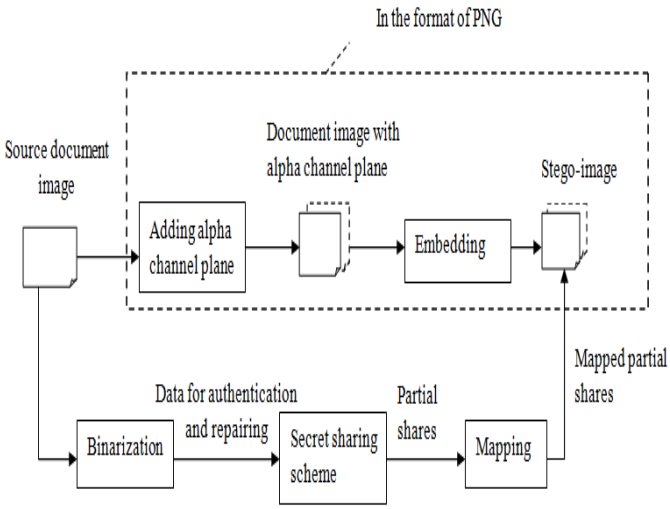


Fig 2:Creating a PNG image from color document image and an Alpha channel

Additionally, once stego-image generated from a conventional method like an LSB-based one is unintentionally compressed by a lossy compression method, the stego-image might cause fake positive alarms in the authentication system. In comparison, the anticipated method yields a stego-image in the PNG format which in usual cases will not be compressed further, reducing the opportunity of invalid authentication caused by imposing undesired compression operations on the stego-image.

GENERATING STEGO-IMAGE

A comprehensive algorithm for describing the generation of a stego-image in the PNG format of the anticipated method is presented as follows:

Algorithm 3:Generating a stego-image in PNG format from a given grayscale image.

Input :A image document in grayscale S with two major grayvalues, and a secret key K.

Output:A stego-image S′ in the PNG format with relevant data embedded, including the authentication signal and the data used for repairing

Step A: Generating authentication signals

(i) (Conversion of Input image to Binary form) Apply moment-preserving threshold [6] to S to obtaintwo representative gray values g1 and g2, compute **$T = (g_1 + g_2)/2$;** And use T as a threshold to convert S into binary form, yielding the binary version $S_b$with "0" representing g_1 and "1" representing g_2

(ii) (Convert the cover image into the PNG format) Convert S into a PNG image with an alpha channel plane$S_\alpha$by creating a new image layer with 100% opacity and no color as $S_\alpha$and combining it with S using an image processing software package.

(iii) Take in an unrefined raster-scan order a 2×3 block $B_b$of S_b with pixels $p_1,p_2\ldots p_6$.

(iv) (Creating authentication signals) Create a 2-bit authentication signal $Z=a_1a_2$with $a_1 = p_1$ XOR p_2XOR p_3 and $a_2= p_4$XOR p_4 XOR p_6. Step B: Design and Embedding of Shares

International Journal of Engineering & Extended Technologies Research (IJEETR)

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

(v) (Creating data for secret sharing) concatenate the 8 bits of a_1, a_2, and $p_1$through p_6 to form an 8-bit string, divide the string into two 4-bit segments, and convert the segments into 2 decimal numbers $m_1$and m_2, respectively.

(vi) (Generation of Partial Share) Set p, c_i, and $x_i$in Eqn. (1) of Algorithm 1 to be the following values:

(a)p = 17(the smallest prime number larger than15);

(b) $d = m_1, c_1 = m_2$;

(c) $x_1 = 1$, $x_2 = 2$, …, $x_6 = 6$; and execute Algorithm 1 as a (2, 6)-threshold secret sharing scheme to generate six partial shares q_1 through q_6 using the following equations:

$$q_i = F(x_i) = (d + c_1 x_i) \bmod p \ldots\ldots \quad (3)$$

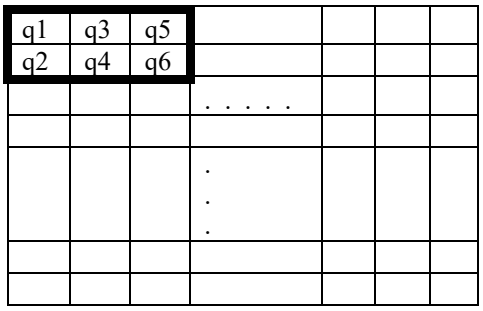
where i = 1, 2… 6.

(vii) (Map of the partial shares) Adding 238 to each of q_1 through q_6, resulting in the new values of q_1', through q_6', respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane S_α.

(viii) (Embedding two fractional shares in the current block) receive the block $B_\alpha$in $S_\alpha$corresponding to $B_b$in S_b, select the first two pixels in B_α in the raster-scan order, and substitute their values by $q_1'$and q_2', respectively.

(ix) (Embedding remaining incomplete shares at random pixels) Use the key K to select randomly 4 pixels in but $S_\alpha$outside B_α, which are unselected yet in this step and not the first 2 pixels of any block, and in the raster scan order replace the four pixels values by the remaining four partial shares q_3' through q_6' generated above, respectively.

(x) If there exists any unprocessed block in S_b, then go to (iii), if not, take the final S in the PNG format as the preferred stego-image S′. The promising values of $q_1$through q_6 yield by Eqn. (3) above are between 0 and 16 because the prime number p used there is 17. After executing (vii) of the above algorithm, they become q_1' through q_6', respectively, which all fall into a small interval of integers ranging from 238 to 254 with a width of 17 (the value of the prime number). Consequent embedding of q_1' through q_6' in such a narrow interval into the alpha channel plane means that very alike values will appear everywhere in the plane, resulting in a nearly uniform transparency effect, which will not stimulate notice from an attacker.



The motivation why we choose the prime number to be 17 in the above algorithm is that if it was chosen instead to be larger than 17, then the above-mentioned interval will be enlarged and the values of q_1' through q_6' will become possibly lesser than 238, creating visually whiter stego-image. In contrast, the 8 bits mentioned in (v) and (vi) above are transformed into 2 decimal numbers m1 and m with their maximum values being 15 (notice (v) above), which are forced to lie in the range of 0 through p-1 (notice Step 2 in Algorithm 1). Therefore, p should not be chosen to be smaller than 16. In short, p = 17 is a best possible choice

6 shares created for a block

2 shares embedded at the current block and 4 at random pixels out of the block

International Journal of Engineering & Extended Technologies Research (IJEETR)

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

q1						
q2						
			. . . . .		q5	
	q6					
			. . .			
		q3				
						q4

Fig 3:Pictorial representation of embedding 6 shares generated for a block, 2 shares embedded in current block and other 4 in 4 randomly selected pixels outside the block, with each selected pixel not being the first 2 ones in any block.

Fig 4:stego image

STEGO-IMAGE AUTHENTICATION

Algorithm 4: Authentication of a given stego-image in the PNG format

Input : A stego-image S′, the representative gray values $g_1$and g_2, and the secret key K used in Algorithm 3.

Output : An image $S_r$with tampered blocks marked, and their data repaired if possible.

Part 1: Extraction of the embedded two representative gray values.

Step 1: (Conversion of the stego-image to Binary form) Compute **$T = (g_1 + g_2)/2$** And use it as a threshold to convert S′ into Binary Form, yielding the binary version Sb′ of S′ with "0" representing g_1 and "1" representing g_2**.**

Part 2: Authentication of the stego-image.

Step 2: (Start looping) Take in a raster-scan order an unprocessed block B_b' from S_b' with pixel values $p_1$through p_6, and find the 6 pixel values q_1' through q_6' of the corresponding block B_b' in the alpha channel plane S_α' of S′.

Step 3: (Drawing out of the secreted authentication signal) to extract the hidden 2-bit authentication signal $Z = a_1a_2$from Bα′ we will follow the steps:

(1) Subtract 238 from each of q1′ and q2′ to obtain the 2 respective partial shares $q_1$and q_2 of B_b'. With the shares (1, q_1) and (2, q_2) as input, perform Algorithm 2 to extract the 2 values d and c1 (the secret and the first coefficient value, respectively) as output. (2) Transform d and c1 into two 4-bit binary values, concatenate them to form an 8-bit string W, and take the first two bits a_1 and a_2 of W to compose the hidden authentication signal $Z = a_1a_2$.

(2) **Step 4**: (Computation of the authentication signal from the current block content) Compute a two-bit authentication signal $Z' = a_1'a_2'$ from the values p_1 through $p_6$of the six pixels of B_b' by $a_1' = p_1 XOR\ p_2\ XOR\ p_3$ and $a_2' = p_4 XOR\ p_5\ XOR\ p_6$.

(3) **Step 5:** (Harmonizing the hidden and computed authentication signals and marking of tampered blocks) Match Z &Z′ by checking if $a_1 = a_1'$ & $a_2 = a_2'$, and if any variance occurs, mark B_b', the corresponding block B′ in S′, and all the partial shares embedded in B'_αtampered.

(4) **Step 6:** (Close loop) if there exists any unprocessed block in S_b', then go to Step 2; otherwise, go on.

International Journal of Engineering & Extended Technologies Research (IJEETR)

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

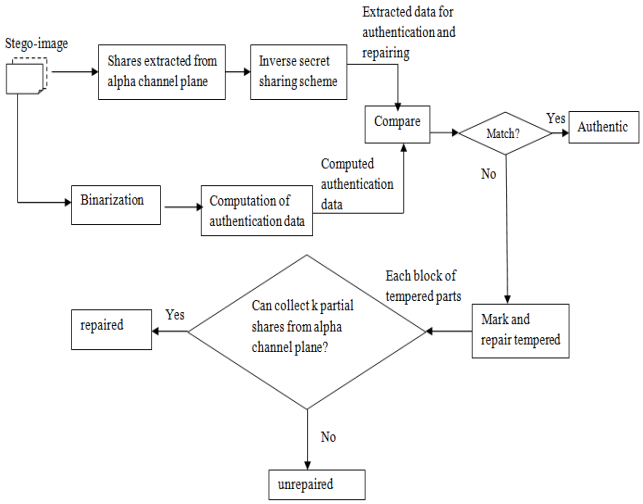


Fig 4:Verification and self-repairing of stego-image in PNG format for the process of image authentication

Part 3: Self-repairing the original image content

Step 7: (Drawing out of the remaining partial shares) For each block B'_{α} in S_{α}, execute the following steps to extract theremaining 4 partial shares q3 through q6 of thecorresponding block B_b' in S_b' from blocks in S_{α}'other thanB$'_{\alpha}$.

Step 8: (Repair the tampered regions) On behalf of each block B′ in S′ marked as tampered previously, execute the following steps to repair it if possible.

(1) From the 6 partial shares $q_1$through q_6 of the block B_b' in S_b' corresponding to B′(two computed in Step 3

(1) and four in Step 7(2) above), select 2 of them, say qk and ql, which are not marked as tampered, if possible.

(2) With the shares (k, q_k) and (l, q_1) as input, execute Algorithm 2 to mine the values of d and c_1(the secret and the first coefficient value) as output.

(3) Transform d and c_1 into two 4-bit binary values and concatenate them to form an 8-bit string W′.

(4) Take the last 6 bits b_1',b_2',… b_6' from W′ and check their binary values to repair the corresponding tampered pixel values y_1', y_2', …, y_6' of block B′ by the following way: if $b_i' = 0$, set $y_i' = g1$; otherwise, set $y_i' = g_2$; where i = 1, 2… 6.

Step 9: Take the final S′ as the desired self-repaired image S_r.

III. MERITS OF THE PROPOSED METHOD

- It provides pixel-level repairs of tampered image parts
- Enhancing data security by secret sharing
- Causing no distortion to the input image
- Use of a new type of image channel for data hiding

IV. CONCLUSION

We have proposed an image authentication method along with a data repair capability for color document images based on secret sharing. Both the generated authentication signal and the content of a block are transformed into partial shares by the Shamir method, which are then distributed in an elegant manner into an alpha channel plane to create a stego-image in the PNG format. For self-repairing the content of a tampered block, the reverse Shamir scheme is used to compute the original content of the block from any 2 un-tampered shares.A measure for enhancing the protection of the data embedded in the alpha channel plane is also proposed.

REFERENCES

1. C. S. Lu and H. Y. M. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Trans. Image Process., vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
2. M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, “Hierarchical watermarking for secure image authentication with localization,” IEEETrans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.
3. Z. M. Lu, D. G. Xu, and S. H. Sun, “Multipurpose image watermarking algorithm based on multistage vector quantization,” IEEE Trans. ImageProcess., vol. 14, no. 6, pp. 822–831, Jun. 2005.

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

4. M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–5,Aug. 2004.
5. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
6. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
7. H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741–744, Dec. 2006.
8. H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.
9. H. Y. Kim and A. A?f, "Secure authentication watermarking for halftone and binary images," Int. J. Imag. Syst. Technol., vol. 14, no.4, pp. 147–152, 2004.
10. Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates," IEICE Trans. Commun., vol. E90-B, no. 11, pp. 3259–3262, Nov. 2007.
11. K.Prakashraj, G.Vijayakumar, S.Saravanan and S.Saranraj, "IoT Based Energy Monitoring and Management System for Smart Home Using Renewable Energy Resources," International Research Journal of Engineering and Technology, Vol.7, Issue 2, pp.1790-1797, 2020.
12. J Mohammed siddi, A. Senthil kumar, S.Saravanan, M. Swathisriranjani, "Hybrid Renewable Energy Sources for Power Quality Improvement with Intelligent Controller," International Research Journal of Engineering and Technology, Vol.7, Issue 2, pp.1782-1789, 2020.
13. T.R. Vignesh, M.Swathisriranjani, R.Sundar, S.Saravanan, T.Thenmozhi," Controller for Charging Electric Vehicles Using Solar Energy", Journal of Engineering Research and Application, vol.10, Issue.01,pp.49-53, 2020.
14. G. Poovarasan, S. Susikumar, S. Naveen, N. Mohananthini, S. Saravanan," Study of Poultry Fodder Passing Through Trolley in Feeder Box," International Journal of Engineering Technology Research & Management, vol.4, Issue.1, pp.76-83, 2020.
15. M.Revathi, S.Saravanan, R.Raja, P.Manikandan," A Multiport System for A Battery Storage System Based on Modified Converter with MANFIS Algorithm," International Journal of Engineering Technology Research & Management, vol.4, issue 2, pp.217-222, 2020.
16. D Boopathi, S Saravanan, Kaliannan Jagatheesan, B Anand, "Performance estimation of frequency regulation for a micro-grid power system using PSO-PID controller", International Journal of Applied Evolutionary Computation (IJAEC), Vol.12, Issue.4, pp.36-49, 2021.
17. V Kumarakrishnan, G Vijayakumar, D Boopathi, K Jagatheesan, S Saravanan, B Anand," Frequency regulation of interconnected power generating system using ant colony optimization technique tuned PID controller", Control and Measurement Applications for Smart Grid: Select Proceedings of SGESC 2021, pp..129-141.
18. G Vijayakumar, M Sujith, S Saravanan, Dipesh B Pardeshi, MA Inayathullaa," An optimized MPPT method for PV system with fast convergence under rapidly changing of irradiation", 2022 International Virtual Conference on Power Engineering Computing and Control: Developments in Electric Vehicles and Energy Sector for Sustainable Future (PECCON), pp.1-4.
19. VM Geetha, S Saravanan, M Swathisriranjani, CS Satheesh, S Saranraj, "Partial Power Processing Based Bidirectional Converter for Electric Vehicle Fast Charging Stations", Journal of Physics: Conference Series, Vol.2325, Issue.1, pp.012028, 2022.
20. M Santhosh Kumar, G Dineshkumar, S Saravanan, M Swathisriranjani, M Selvakumari, "Converter Design and Control of Grid Connected Hybrid Renewable Energy System Using Neuro Fuzzy Logic Model", 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), pp.1-6, 2022.
21. C Gnanavel, A Johny Renoald, S Saravanan, K Vanchinathan, P Sathishkhanna, "An Experimental Investigation of Fuzzy-Based Voltage-Lift Multilevel Inverter Using Solar Photovoltaic Application", Smart Grids and Green Energy Systems, pp.59-74, 2022.
22. V Kumarakrishnan, G Vijayakumar, D Boopathi, K Jagatheesan, S Saravanan, B Anand, "Optimized PSO technique based PID controller for load frequency control of single area power system", Solid State Technology, Vol.63. Issue.5, pp.7979-7990, 2020.
23. G. Poovarasan, S. Susikumar, S. Naveen, N. Mohananthini, S. Saravanan, "Implementation of IoT Based Poultry Feeder Box", International Journal of Innovative Research In Technology, Vol.6, Issue.2, pp.33-38, 2020.
24. N.Gokulnath, B.Jasim Khan, S.Kumaravel, Dr.A.Senthil Kumar and Dr.S.Saravanan, "Soldier Health and Position Tracking System", International Journal of Innovative Research In Technology, Vol-6 Issues 12, pp.39-45, 2020.

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

25. P.Navaneetha, R.Ramiya Devi, S.Vennila, P.Manikandan and Dr.S.Saravanan, " IOT Based Crop Protection System against Birds and Wild Animal Attacks", International Journal of Innovative Research In Technology, Vol-6 Issues 11, pp.133-143, 2020.
26. K. Punitha, M. Rajkumar, S. Karthick and Dr. S. Saravanan, " Impact of Solar And Wind Integration on Frequency Control System", International Research Journal of Engineering and Technology, Vol 7 Issue 3, pp.1357-1362,2020.
27. A.Arulkumar, S.Balaji, M.Balakrishnan, G.Dineshkumar and S.Saravanan, "Design And Implementation of Low Cost Automatic Wall Painting Machine" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.170-176, 2020.
28. V.Periyasamy, S.Surya, K. Vasanth, Dr.G.Vijayakumar and Dr.S.Saravanan, "Design And Implementation of Iot Based Modern Weaving Loom Monitoring System" International Journal of Engineering Technology Research & Management, Vol-4 Issues 04, pp.11-18, 2020.
29. M.Yogheshwaran, D.Praveenkumar, S.Pravin, P.M.Manikandan and Dr.S.Saravanan, "IoT Based Intelligent Traffic Control System" International Journal of Engineering Technology Research & Management, Vol-4 Issues 04, pp.59-63, 2020.
30. R.Pradhap, R.Radhakrishnan, P.Vijayakumar, R.Raja and Dr.S.Saravanan, "Solar Powered Hybrid Charging Station For Electrical Vehicle" International Journal of Engineering Technology Research & Management, Vol-4 Issues 04, pp.19-27, 2020.
31. .Shenbagavalli, T.Priyadharshini, S.Sowntharya, P.Manikandan and Dr.S.Saravanan, "Design and Implementation of Smart Traffic Controlling System" International Journal of Engineering Technology Research & Management, Vol-4 Issues 04, pp.28-36, 2020.
32. M.Pavithra, S.Pavithra, R.Rama Priya, M.Vaishnavee, M.Ranjitha and S.Saravanan, "Fingerprint Based Medical Information System Using IoT" International Journal of Engineering Technology Research & Management, Vol-4 Issues 04, pp.45-51, 2020.
33. A.Ananthan, A.M.Dhanesh, J.Gowtham, R.Dhinesh, G.Jeevitha and Dr.S.Saravanan, "IoT Based Clean Water Supply" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.154-162, 2020.
34. R.Anbarsan, A.Arsathparvez, K.S.Arunachalam, M.Swathisriranjani and Dr.S.Saravanan, "Automatic Class Room Light Controlling Using Arduino" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.192-201, 2020.
35. S.Karthikeyan, A.Krishnaraj, P.Magendran, T.Divya and Dr.S.Saravanan , "The Dairy Data Acquisition System" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.163-169, 2020.
36. M.Amaran, S.Mannar Mannan, M.Madhu, Dr.R.Sagayaraj and Dr. S.Saravanan, "Design And Implementation of Low Cost Solar Based Meat Cutting Machine" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.202-208, 2020.
37. N.Harish, R.Jayakumar, P.Kalaiyarasan, G.Vijayakumar and S. Saravanan, "IoT Based Smart Home Energy Meter" International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.177-183, 2020.
38. K.Subashchandrabose, G.Moulieshwaran, M.Raghul, V.Dhinesh and S.Saravanan, "Design of Portable Sanitary Napkin Vending Machine", International Journal of Engineering Technology Research & Management, Vol-4 Issues 03, pp.52-58, 2020.
39. D.Hemalatha, S.Indhumathi, V.Myvizhi and S.Saravanan, "Design and Implementation of Intelligent Controller for Domestic Applications", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.4-7, 2023.
40. S. Divyasri, E. Indhu, M. P. Keerthana, M. Selvakumari and S. Saravanan, "Gas Cylinder Monitoring System using IoT", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.67-71, 2023.
41. J.Arul, R.Balaji, S.Jeyamoorthy, M.Manipathra, R.Sundar and S.Saravanan, "IoT based Air Conditioner Control using ESP32", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.48-52, 2023.
42. Vundel Munireddy, J.Prahathesvaran, C.R.Thirunavukarasu, M.Santhosh Kumar and S.Saravanan, "IoT Based Charge Controller for Direct Fast Charging of Electric Vehicles Using Solar Panel", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.77-81, 2023.
43. D.Monish Kumaar, K.Akash, S.Aswinkumar, S.Saravanan and R. Sagayaraj, "IoT based Industry Surveillance and Air Pollution Monitoring using Drones", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.14-18, 2023.
44. T.Silambarasan, R.Surya, J.Pravinkumar, R.Sundar and S Saravanan, "IoT based Monitoring System For Sewage Sweeper", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.88-93, 2023.

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

45. R.Aravinthan, Alwin.Augustin, P.Divagaran, S.Saravanan and P.Manikandan, "IoT Based Power Consumption and Monitoring System", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.43-47, 2023.
46. S.Partheeban, S.Sundaravel, S.Umapathi, R.Sagayaraj and S.Saravanan, "IoT based Safety Helmet for Mining Workers", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.116-120, 2023.
47. K.Eswaramoorthi, R.Manikandan, R.Balamurugan, C.Ramkumar and S.Saravanan, "Smart Parking System using IoT", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.53-57, 2023.
48. S.Nirmalraj, C.Pranavan, M.Prem and S.Saravanan, "Smart Trolley With IoT Based Billing System", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.111-115, 2023.
49. V.Gunasekaran, M.Gowtham , S. Anbubalaji, S.Saravanan and R.Prakash, "Solar based Electric Wheel Chair", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.8-13, 2023.
50. P Thava Prakash, P.Venketesan, D.Vignesh, S.Prakash, S.Saravanan, "Design of Low Cost E-Bicycle using Brushless DC Motor with Speed Regulator", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.148-153, 2023.
51. D.Tamilarasan, V.S.Vairamuthu, Y.Vasanth, K.Umadevi, S.Saravanan, "GSM based Agricultural Motor Control", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.172-177, 2023.
52. P. Vimal, S.Veerasigamani, R.Srihari, C.S.Satheesh, S.Saravanan, "IoT Based Optimal Power Management System For Smart Grid", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.160-165, 2023.
53. S.Abimanyu, P.Jagadheeswaran, S.Jaganath, K.Sanjay, R.Sivapranesh, K.Velmurugan, N.Mohananthini, C.S.Satheesh, S.Saravanan, "Portable Solar Tree", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.154-159, 2023.
54. M.Karthikeyan, S.Bilalahamad, V.A.Chandru, V.Deepika and S.Saravanan, "Design and Development of IoT based Motor Starter", International Journal of New Innovations in Engineering and Technology, Vol.22, Issue.3, pp.178-183, 2023.
55. R.Anbarsan, A.Arsathparvez, K.S.Arunachalam, M.Swathisriranjani and S.Saravanan, "Automatic Class Room Light Controlling Using Arduino" International Journal of Engineering Technology Research & Management (IJETRM), Vol-4 Issues 03, pp.192-201, 2020.
56. S.Karthikeyan, A.Krishnaraj, P.Magendran, T.Divya and S.Saravanan , "The Dairy Data Acquisition System" International Journal of Engineering Technology Research & Management (IJETRM), Vol-4 Issues 03, pp.163-169, 2020.
57. N.Harish, R.Jayakumar, P.Kalaiyarasan, G.Vijayakumar and S. Saravanan, "IoT Based Smart Home Energy Meter" International Journal of Engineering Technology Research & Management (IJETRM), Vol-4 Issues 03, pp.177-183, 2020.
58. G. Poovarasan, S. Susikumar, S. Naveen, N. Mohananthini, S. Saravanan," Study of Poultry Fodder Passing Through Trolley in Feeder Box," International Journal of Engineering Technology Research & Management, vol.4, Issue.1, pp.76-83, 2020.
59. A.Ananthan, A.M.Dhanesh, J.Gowtham, R.Dhinesh, G.Jeevitha and S.Saravanan, "IoT Based Clean Water Supply" International Journal of Engineering Technology Research & Management (IJETRM), Vol-4 Issues 03, pp.154-162, 2020.
60. Ram Kumar C, Saravanan S, and Nagarajan C,"Hybrid LSTM and Deep Reinforcement Learning for Autonomous Battery Health Optimization in Electric Vehicles", Electrical Power Systems Research, Vol-253 Issues 112535, ISSN No:0378-7796,2025.
61. Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.
62. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.
63. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
64. Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).
65. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

66. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
67. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
68. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
69. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
70. Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).
71. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
72. Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.
73. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
74. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
75. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
76. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
77. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
78. Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
79. Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
80. Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
81. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
82. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
83. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
84. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
85. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
86. Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
87. Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.

N: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, Ma1rch - April 2026 |

DOI:10.15662/IJEETR.2026.0802337

88. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
89. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
90. SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.
91. Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).
92. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
93. Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
94. Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
95. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.