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.2026.0802352

Development of an Automatic Smart Milking Machine using Solar

Dr.S.Saravanan,Mrs.G.Jeevitha, Shanmugapriya T, Snega K, Sruthi R, Thanuja S, Nandhini L

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: Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, we study data delivery mechanisms that can with high probability circumvent black holes formed by these attacks. We argue that classic multipath routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once the adversary acquires the routing algorithm, it can compute the same routes known to the source, hence making all information sent over these routes vulnerable to its attacks. In this paper, we develop mechanisms that generate randomized multi-path routes. Under our designs, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet.

KEYWORDS: Automatic Milking Machine, Solar Energy System, Wireless Sensor Networks, Randomized Multi-path Routing, Data Security, IoT-based Automation, Energy Efficiency

I. INTRODUCTION

1.1 Motivations

Of the various possible security threats encountered in a wireless sensor network (WSN), in this paper we are specifically interested in combating two types of attacks: compromised-node (CN) and denial-of-service (DOS). In the CN attack, an adversary physically compromises a subset of nodes to eavesdrop information, whereas in the DOS attack, the adversary interferes with the normal operation of the network by actively disrupting, changing, or even paralyzing the functionality of a subset of nodes. These two attacks are similar in the sense that they both generate *black holes*: areas within which the adversary can either passively intercept or actively block information delivery. Due to the unattended nature of WSNs, adversaries can easily produce such black holes. Severe CN and DOS attacks can disrupt normal data delivery between sensor nodes and the sink, or even partition the topology. In practice, due to the difficulty of acquiring such location information, the above idea is implemented in a probabilistic manner, typically through a two-step process. First, the packet is broken into *M shares* (i.e., components of a packet that carry partial information) using a (*T;M*)-threshold secret-sharing mechanism such as the Shamir's algorithm. The original information can be recovered from a combination of at least *T* shares, but no information can be guessed from less than *T* shares. Second, multiple routes from the source to the destination are computed according to some multi-path routing algorithm. These routes are node-disjoint or maximally node-disjoint subject to certain constraints (e.g., min-hop routes). The *M* shares are then distributed over these routes and delivered to the destination. As long as at least $M_i T$ +1 (or *T*) shares bypass the compromised (or jammed) nodes, the adversary cannot acquire (or deny the delivery of) the original packet. We argue that three security problems exist in the above counter-attack approach.

First, this approach is no longer valid if the adversary can *selectively* compromise or jam nodes. This is because the route computation in the above multi-path routing algorithms is deterministic in the sense that for a given topology and given source and destination nodes, the same set of routes are always computed by the routing algorithm. As a result, once the routing algorithm becomes known to the adversary (this can be done, e.g., through memory interrogation of the compromised node), the adversary can compute the set of routes for any given source and destination. Then the adversary can pinpoint to one particular node in each route and compromise (or jam) these nodes.

1.2 Contributions and Organization

The key contributions of this work are as follows:

1. We explore the potential of random dispersion for information delivery in WSNs. Depending on the type of information available to a sensor, we develop four distributed schemes for propagating information "shares":vpurely random propagation (PRP), directed random

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

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

DOI:10.15662/IJEETR.2026.0802352

propagation (DRP), non-repetitive random propagation (NRRP), and multicast tree-assisted random propagation (MTRP). PRP utilizes only one-hop neighbourhood information and provides baseline performance. DRP utilizes two-hop neighborhood information to improve the propagation efficiency, leading to a smaller packet interception probability. The NRRP scheme achieves a similar effect, but in a different way: it records all traversed nodes to avoid traversing them again in the future. MTRP tries to propagate shares in the direction of the sink, making the delivery process more energy efficient.

2. We theoretically evaluate the goodness of these dispersive routes in terms of avoiding black holes. We conduct asymptotic analysis (i.e., assuming an infinite number of nodes) for the worst-case packet interception probability and energy efficiency under the baseline PRP scheme. Our results can be interpreted as the performance limit of PRP, and a lower-bound on the performance of the more advanced DRP, NRRP, and MTRP schemes. Our analysis helps us better understand how security is achieved under dispersive routing. Based on this analysis, we investigate the tradeoff between the random propagation parameter and the secret sharing parameter. We furtheroptimize these parameters to minimize the end-to-end energy consumption under a given security constraint.

3. We conduct extensive simulations to study the performance of the proposed schemes under more realistic settings. Our simulation results are used to verify the effectiveness of our design. When the parameters are appropriately set, all four randomized schemes are shown to provide better security performance at a reasonable energy cost than their deterministic counterparts. At the same time, they do not suffer from the type of attacks faced by deterministic multi-path routing.

II. RANDOMIZED MULTI-PATH DELIVERY

2.1 Overview

We consider a 3-phase approach for secure information delivery in a WSN: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., minhop routing) toward the sink. More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares according to a $(T;M)$-threshold secret sharing algorithm, e.g., Shamir's algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on.

In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. When the TTL value reaches 0, the last node to receive this share begins to route it towards the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares.

The effect of route dispersiveness on bypassing black holes is illustrated in Figure 2, where the dotted circles represent the ranges the secret shares can be propagated to in the random propagation phase. A larger dotted circle implies that the resulting routes are geographically more dispersive.

Comparing the two cases in Figure 2, it is clear that the routes of higher dispersiveness are more capable of avoiding the black hole. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

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.2026.0802352

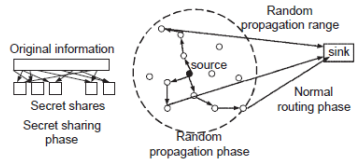

Fig. 1. Randomized dispersive routing in a WSN.

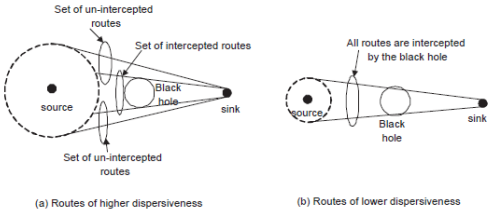

Fig. 2. Implication of route dispersiveness on bypassing the black hole.

2.2 Random propagation of Information Shares

To diversify routes, an ideal random propagation algorithm would propagate shares as dispersively as possible. Typically, this means propagating the shares farther from their source. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. The challenge here lies in the random and distributed nature of the propagation: a share may be sent one-hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security standpoint. To tackle this issue, some control needs to be imposed on the random propagation process.

In PRP, shares are propagated based on one-hop neighbourhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbour list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it towards the sink using normal min-hop routing. The WANDERER scheme is a special case of PRP with $N = 1$. The main drawback of PRP is that its propagation efficiency can be low, because a share may be propagated back and forth multiple times between neighboring hops.

2.2.2 Non-repetitive Random Propagation NRRP is based on PRP, but it improves the propagation efficiency by reording the nodes traversed so far. Specifically, NRRP adds a "node-in-route" (NIR) field to the header of each share. Initially, this field is empty. Starting from the source node, whenever a node propagates the share to the next hop, the id of the up-stream node is appended to the NIR field. Nodes included in NIR are excluded from the random pick at the next hop. This non-repetitive propagation guarantees that the share will be relayed to a different node in each step of random propagation, leading to better propagation efficiency.

2.2.3 Directed Random Propagation

DRP improves the propagation efficiency by using twohop neighborhood information. More specifically, DRP adds a "last-hop neighbor list" (LHNL) field to the header of each share. Before a share is propagated to the next node, the relaying node first updates the LHNL field with its neighbor list. When the next node receives the share, it compares the LHNL field against its own neighbor list, and randomly picks one node from its neighbors that are not in the LHNL. It then decrements the TTL value, updates the LHNL field, and relays the share to the next hop, and so on. Whenever the LHNL fully overlaps with or contains the relaying node's neighbour list, a random neighbor is selected, just as in the case of the PRP scheme.

2.2.4 Multicast Tree-assisted Random Propagation MTRP aims at actively improving the energy efficiency of random propagation while preserving the dispersiveness of DRP. The basic idea comes from the following observation of Figure 1: Among the 3 different routes taken by shares, the route on the bottom right is the most energy efficient

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.2026.0802352

because it is the shortest end-to-end path. So, in order to improve energy efficiency, shares should be best propagated in the direction of the sink.

III. ASYMPTOTIC ANALYSIS OF THE PRP SCHEME

The random routes generated by the four algorithms in Section 2 are not necessarily node-disjoint. So a natural question is how good these routes are in avoiding black holes. We answer this question by conducting asymptotic analysis of the PRP scheme. Theoretically, such analysis can be interpreted as an approximation of theperformance when the node density is sufficiently large. It also serves as a lower bound on the performance of the NRRP, DRP, and MTRP schemes. Note that the security analysis for the CN and DOS attacks are similar because both of them involve calculating the packet interception probability. For brevity, we only focus on the CN attack model. The same treatment can be applied to the DOS attack with a straightforward modification.

3.1 Network and Attack Models

We consider an area *S* that is uniformly covered by sensors with density ½. We assume a unit-disk model for the sensor communication, i.e., the transmitted signal from a sensor can be successfully received by any sensor that is at most *Rh* meters away. Multi-hop relay is used if the intended destination is more than *Rh* away from the source. We assume that link-level security has been established through a conventional cryptography-based bootstrapping algorithm.

3.2 Security Definition

For a given source sensor node, the security provided by the protocol is defined as the worst-case (maximum) probability that for the *M* shares of an information packet sent from the source, at least *T* of them are intercepted by the black hole. Mathematically, this is defined as follows. Let the distance between the source *s* and the sink *o* be *ds*. As shown in Figure 3, we define a series of *N*+1 circles co-centered at *s*. For the *i*th circle, 1 · *i* · *N*, the radius is *iRh*. For circle 0, its radius is 0. These *N* +1
circles will be referred to as the *N-hop neighborhood* of *s*. More specifically, we say that a node is *i* hops away from *s* if it is located within the intersection between circles *i ¡* 1 and *i*. We refer to this intersection as ring *i*. For an arbitrary share, after the random propagation phase, the id of the ring in which the last receiving node, say *w*, is located is a discrete random variable *»* with state space *f*1*; : : : ;Ng*. The actual path from *w* to the sink is decided by the specific routing protocol employed by the network. Accordingly, different packet interception rates are obtained under different routing protocols. However, the route given by min-hop routing, which under high node density can be approximated by the line between *w* and the sink, gives an upper bound on the packet interception rates under all other routing protocols. This can be justified by noting that min-hop routing tends not to distribute traffic over various intermediate nodes and only selects those nodes that are closest to the sink.As illustrated in Figure 3, this path-concentration effect makes min-hop routing have a smaller traversing area of the paths, and thus is more prone to packet interception, especially when compared to power-balancing routing protocols that build dispersive routes. The interception probability for an arbitrary share of information is given by

$$\begin{aligned} P_I &= \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\text{Area of ring } i} \\ &= \sum_{i=1}^{N} \Pr\{\xi = i\} \frac{S_i}{\pi i^2 R_h^2 - \pi (i-1)^2 R_h^2}. \end{aligned} \quad (1)$$

Accordingly, the worst case probability that at least *T* out of *M* shares are intercepted by *E* is given by

$$P_S^{(\max)} = \sum_{k=T}^{M} \binom{M}{k} P_I^k (1 - P_I)^{M-k} \quad (2)$$

To proceed with the security analysis, we need to calculate the shaded area in each ring *Si*

3.3 Derivation of the Packet Interception Area

The derivation of *Si* falls into one of the following three cases:

Case 1: When *iRh*< *Reds/de* (e.g., rings 1 to 3 in Figure 3), ring *i* is completely covered by the shaded region. Therefore,

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.2026.0802352

$$S_i^{(case\ 1)} = \pi[i^2 - (i-1)^2]R_h^2, 1 \le i \le \left\lfloor \frac{R_e d_s}{R_h d_e} \right\rfloor \quad (3)$$

Case 2: When $(i ¡ 1)Rh < Reds\ de < iRh$, as shown in Figure 4, ring i is partially shaded. The shaded area of ring i is the intersection of circle i and the cone CoD minus the area of circle $i¡1$. The area of this intersection is composed of three components: the trapezoid $A1$ ($B1B2B3B4$), two circle segments $A2$ (surrounded by arch $B1B5B2$ and chord $B1B2$), and $A3$ (surrounded by arch $B3B6B4$ and chord $B3B4$). It can be shown that $A1$ has a height $hA1 = x1 ¡ x2$ where

$$x_1 \stackrel{\text{def}}{=} \frac{R_e^2 d_s + \sqrt{R_e^4 d_s^2 - d_e^2 R_2^2 d_s^2 + d_e^4 i^2 R_h^2 - i^2 d_e^2 R_h^2 R_e^2}}{d_e^2} \quad (4)$$

$$x_2 \stackrel{\text{def}}{=} \frac{R_e^2 d_s - \sqrt{R_e^4 d_s^2 - d_e^2 R_2^2 d_s^2 + d_e^4 i^2 R_h^2 - i^2 d_e^2 R_h^2 R_e^2}}{d_e^2}. \quad (5)$$

The lengths of the two parallel edges of $A1$ are given by

$$l_1 = 2\left(-\frac{R_e}{\sqrt{d_e^2 - R_e^2}}x_1 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}}\right) \quad (6)$$

$$l_2 = 2\left(-\frac{R_e}{\sqrt{d_e^2 - R_e^2}}x_2 + \frac{R_e d_s}{\sqrt{d_e^2 - R_e^2}}\right). \quad (7)$$

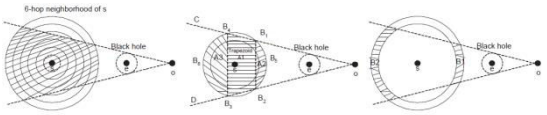

Fig. 3. Packet-interception area, a 6-hop random propagation example. Fig. 4. Packet-interception area: case 2. Fig. 5. Packet-interception area: case 3.

Therefore, the area of $A1$ is given by

$$S_i^{(A_1)} = \frac{(l_1 + l_2)h_{A_1}}{2}.$$

The area of $A2$ and $A3$ are given by

$$S_i^{(A_2)} = (iR_h)^2 \arctan\left(\frac{0.5l_1}{x_1}\right) - 0.5x_1 l_1$$

$$S_i^{(A_3)} = (iR_h)^2 \arctan\left(-\frac{0.5l_2}{x_2}\right) + 0.5x_2 l_2.$$

Energy Efficiency of the Random Propagation

We assume that the energy consumption for delivering one bit over one hop is a constant q. Then the average energy consumption for delivering one packet from source s to sink o depends on the average length (in hops) of the route. Note that each random route consists of two components. The first is a fixed Nhop component attributed to the random propagation operation. The second component involves sending the share from the last random relay node, i.e., w, to the sink o using a normal single path routing. Under the asymptotic assumption, when min-hop routing is used, the ratio between the number of hops from w ! o and from s ! o can be approximated by the ratio of the lengths of these two paths.

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.2026.0802352

IV. SIMULATION STUDIES

4.1 Simulation Setup

In this section, we use simulation to evaluate the performance of PRP, NRRP, DRP, and MTRP under more realistic settings. To better understand the capability of these randomized multi-path routing algorithms in bypassing black holes, we also compare their performance against a deterministic counterpart, H-SPREAD , which generates node-disjoint multi-path routes to combat CN attack in WSNs.

4.2 Simulation Results

4.2.1 Single-source Case

We first fix the location of the source node at (¡50; 0). we plot the packet interception probability as a function of the TTL value (N) and the number of shares (M) that each packet is broken into, respectively.

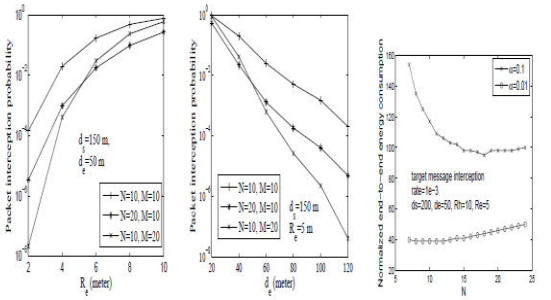

Fig. 11. Packet interception probability vs. black hole size.

Fig. 12. Packet interception probability vs. black hole location.

Fig. 13. Energy consumption under different (N, M).

The packet interception probability calculated according to our asymptotic analytical model for PRP is also plotted in the same figure for comparison. These figures show that increasing N and M helps reduce the packet interception probability for all proposed schemes.

V. RELATED WORK

The concept of multi-path routing dates back to 1970s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement. Later on, one of its sub-classes, *path-disjoint* multi-path routing, has attracted a lot of attention in wireless networks due to its robustness in combating security issues. The related work can be classified into three categories. As pointed out in , actually very limited number of node-disjoint paths can be found when node density is moderate and the source is far away from the destination. Furthermore, the security issue is not accounted for explicitly in this category of work.

VI. CONCLUSIONS

Our analysis and simulation results have shown the effectiveness of the randomized dispersive routing in combating CN and DOS attacks. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to as low as 10¡3, which is atleast one order of magnitude smaller than approaches that use deterministic node-disjoint multi-path routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy.

REFERENCES

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, Aug. 2002.
2. C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In *Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA)*, pages 122–131, 2003.
3. M. Burmester and T. V. Le. Secure multipath communication in mobile ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, pages
4. 405–409, 2004.

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

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

DOI:10.15662/IJEETR.2026.0802352

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. T. Claveirole, M. D. de Amorim, M. Abdalla, and Y. Viniotis. Securing wireless sensor networks against aggregator compromises. *IEEE Communications Magazine*, pages 134–141, Apr. 2008.
8. D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, pages 139–172. Addison- Wesley, 2001.
9. P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing. In *Proceedings of the IEEE INFOCOM Conference*, pages 1952–1963, Mar. 2005.
10. P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.
11. S. J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In *Proceedings of the IEEE ICC Conference*, pages 3201–3205, 2001.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.

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

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

DOI:10.15662/IJEETR.2026.0802352

26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. S.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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.

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

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

DOI:10.15662/IJEETR.2026.0802352

46. 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.
47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.
59. 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.
60. 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.
61. 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.
62. 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.
63. 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.
64. 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.
65. 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).
66. 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.

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

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

DOI:10.15662/IJEETR.2026.0802352

67. 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.
68. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
69. 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.
70. 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.
71. 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).
72. 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.
73. 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.
74. 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.
75. 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.
76. 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.
77. 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.
78. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
79. 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.
80. 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.
81. 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.
82. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
83. 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.
84. 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.
85. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
86. 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.
87. 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.
88. 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.

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

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

DOI:10.15662/IJEETR.2026.0802352

89. 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.
90. 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.
91. 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.
92. 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).
93. 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.
94. 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.
95. 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.
96. 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.