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.2026.0802353

Smart Solar Baby Incubator with Real – Time IoT Monitoring

Dr.S.Saravanan, Mrs.S.Rajeswari, Dharshini N, Swetha G, Swetha G, Priyanka K, Kaviya S, Prithika M

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: Network firewall is used to protect our network against unwanted malicious targeting on internet server. Incoming and outgoing Internet traffic is inspected by network firewalls. Based on a set of rules, firewalls can allow or block incoming or outgoing traffic, where each rule represents a set of conditions. That rule interrogates incoming packets sequentially rule by rule until a match is found. If an incoming packet matches all conditions of a particular rule, then a certain action is taken, e.g., to pass or drop the packet. A packet can match the conditions of more than one rule. In such a case, the first rule will have priority and its action will be applied to the packet. Analytical model based on systematic approach is used to identify the performance of rule-based firewall, when subjected to normal flow attack and Dos flow attack and can verify and validate the model. Using systematic approach to estimate the performance offered by stateful firewall. A stateful firewall secures a network by keeping track of flow and enforcing security policies. A stateful firewall inspects all incoming and outgoing packets and decides to discard or accept a packet based on the sequence of rules in the firewall rule set and its session table. Specifically, to study and analyze the performance of firewalls when implementing the mitigation solution of real time dynamic re-ordering of the ruleset in which frequently triggered rules are placed on the top of the ruleset.

KEYWORDS: Network Firewall, DoS Attack, Analytical Model, Stateful Firewall

I. INTRODUCTION

Network firewall is used to protect our network against unwanted malicious targeting on internet server. Firewalls themselves can be subjected to malicious attacks from the Internet as they are typically deployed at the edge of the network. Firewalls are typically deployed at the edge of the network or at the entry point of a private network. Incoming and outgoing internet traffics inspected by network firewalls. Based on a set of rules, firewalls can allow or block incoming or outgoing traffic. Network firewalls have a rule-based engine that interrogates incoming packets sequentially rule by rule until a match is found. If an incoming packet matches all conditions of a particular rule, then a certain action is taken, eg. to pass or drop the packet. A packet can match the conditions of more than one rule. In such a case, the first rule will have priority and its action will be applied to the packet. Accordingly, the firewall checks the rules sequentially, one by one, until a rule is matched. According to the 2010Report conducted by Arbor Networks, there is a staggering and alarming 102 percent increase of DDoS attack bandwidth in 2010 when compared to 2009 [1]. The increase of this bandwidth has been attributed to the exponential growth of botnets from which such attacks originate.

The general reasoning behind firewall usage is that without a firewall, a subnet's systems expose themselves to inherently insecure services such as NFS or NIS and to probes and attacks from hosts elsewhere on the network. In a firewall less environment, network security relies totally on host security and all hosts must, in a sense, cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords. A firewall approach provides numerous advantages to sites by helping to increase overall host security.

A firewall can either be software based or hardware based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

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

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

DOI:10.15662/IJEETR.2026.0802353

There are two basic ways to create firewall ruleset: “inclusive” or “exclusive”. An exclusive firewall allows all traffic through except for the traffic matching the ruleset. An inclusive firewall does the reverse. It only allows traffic matching the rules through and blocks everything else. An inclusive firewall offers much better control of the outgoing traffic, making it a better choice for systems that offer services to the public Internet. It also controls the type of traffic originating from the public Internet that can gain access to your private network. All traffic that does not match the rules are blocked and logged by design. Inclusive firewalls are generally safer than exclusive firewalls because they significantly reduce the risk of allowing unwanted traffic to pass through them.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

II. RELATED WORK

Acharya, et al. in [2] developed a simulation framework to study and analyze firewall operations in order to improve its performance against dynamically changing network traffic characteristics. In [3] and [4], an experimental evaluation of firewall performance is presented using firewall analysis tools. Some work has also been done on the analysis of firewalls vulnerability to traffic-specific attacks, such as IP spoofing attacks [5]. In [6], performance metrics for vulnerabilities resulting from firewall operations are presented and analyzed. In [7], a trace route technique was used to determine whether or not a particular packet can pass from an outside remote host to a destination host behind a firewall.

Our analytical model can be used to analyze firewall performance when the firewall is subjected to normal traffic flows as well as DoS attack flows. The performance can be analyzed when launching DoS attack flows targeting top and bottom rules. Analyzing the performance of a firewall when targeting bottom rules is of a paramount importance to network designers and security engineers to assess the resiliency of the firewall against worst-case DoS attacks. It was shown in [8] that bottom rules can be remotely discovered by an outside attacker. An attacker then can launch a complexity algorithmic attack that primarily target bottom rules, and effectively degrading rapidly the performance of a firewall with a low-rate DoS attack flow. Complexity-algorithmic attacks, which have been first described in [9], are a class of low-rate DoS attacks that exploit algorithmic deficiencies in software design.

The key component of a firewall configuration is the access control list (ACL). An ACL consists of an ordered list of rules, each with a predicate that describes which packets are matched by this rule and the action to be taken on matched packets. Contemporary firewalls provide numerous actions: a packet may be dropped, accepted, sanitized, transformed, logged, and nearly any combination thereof. A rule-based firewall maps the logic specified in the ACL to a list data structure. A packet is compared with each rule successively in the sequence until the first matching rule is found, and the action for this rule is taken on the packet. Many firewall implementations have slightly different semantics, such as last matching, last with first matching, and conditional subsequences [10]. Rule-based firewalls, with popular models such as Cisco System’s PIX firewall, Linux’s Netfilter and the BSD Packet Filter, are widely used in production networks.

Firewalls are core elements in network security. However, managing firewall rules, especially for enterprize networks, has become complex and error-prone. Firewall filtering rules have to be carefully written and organized in order to correctly implement the security policy. The filtering decision is taken according to a set of ordered filtering rules.A firewall is a network element that controls the traversal of packets across the boundaries of a secured network based on a specific security policy. A firewall security policy is a list of ordered rules that define the actions performed on network packets based on specific filtering conditions. A rule is composed of set of filtering fields (also called network fields) such as protocol type, source and destination IP addresses and ports, as well as an action field. The filtering fields of a rule represent the possible values of the corresponding fields in actual network traffic that matches this rule. Each network field could be a single value or range of values. Filtering actions are either to accept, which permits the packet into or from the secure network, or to deny, which causes the packet to be blocked. The packet is permitted or

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

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

DOI:10.15662/IJEETR.2026.0802353

blocked by a specific rule if the packet header information matches all the network fields of this rule. Otherwise, the following rule is examined and the process is repeated until matching rule is found or the default policy action is performed[11].

III. PROPOSED METHODOLOGY

A Problem Statement

The model can be used to measure the performance when the firewall is subjected to normal traffic flows as well as DoS attack flows targeting different rule positions. It was demonstrated that targeting rules at the bottom of a relatively large ruleset can be severely detrimental to the performance of the firewall. As a good design practice and vital countermeasure against DoS attacks that target bottom rules, it is recommended to minimize the size of the firewall ruleset or to rearrange dynamically rules so that bottom rules can be served at the top of the ruleset, thereby making it harder to launch such complexity algorithmic attacks that target bottom-rules.

B. MAC Algorithm

MAC Algorithm is responsible for encrypting the message is called message digest algorithms. The most common two message digest algorithms are MD5 and SHA-1algorithm.

C.Md5 Algorithm

The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input.

D.SHA-1Algorithm.

Message Digest is an constructor-Creates a message digest (Encrypted form) with the specified algorithm name. When a message of any length $< 2^{64}$ bits is input, the SHA-1 produces a 160-bit output called a message digest. The implementation of these message digest algorithms to compute a hash value for the message (that is, 128-bit digest with MD5 and 160-bit digest with SHA-1) The sender encrypt the message digest with his private key. Then the recipient can decrypt the encrypted message digest with the sender's public key.

Step 1: MessageDigest md = MessageDigest.getInstance
("SHA-1");
Generates a MessageDigest object(md) that implements the specified digest algorithm getInstance is used to get the specified algorithm in corresponding default package.

Step 2: byte messageDigest[] = md.digest();

Step 3: Digest()-Completes the hash computation by performing final operations such as padding.

```
Store that result into byte form.
StringBuffer buffer = new StringBuffer();

for (int i = 0; i < messageDigest.length; i++)
{
 buffer.append(Integer.toHexString(0xFF &  [i]));
}
 return buffer.toString();
```

Step 4:Read the message in messagedigest and convert this to hexadecimal form and then return the value in string format.

E. LZ77 compression

Prefix Compression:

Its principles are simple, however this algorithm tends to be difficult to implement.Instead of keeping all these words in plain text or transferring all them over a network, we can compress (encode) them with prefix encoding. It's clear that each of these words begins with the prefix "use" which is also the first word from the list.

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.2026.0802353

```
1:  begin
2:  fill view from input
3:  while (view not empty) do
4:  begin
5:  find longest prefix p of view starting in coded part
6:  i := position of p in window
7:  j := length of p
8:  X := first char after p in view
9:  output(i,j,X)
10: add j+1 chars
11: end
12: end
```

This method uses window divided to search buffer and look-ahead buffer. Size of the search buffer is usually 8 192 bits and size of the look-ahead buffer about 10 to 20 bits. In demonstration both parameters can be set.

The algorithm can be described as follows. First the longest prefix of a look-ahead buffer that starts in search buffer is found. This prefix is encoded as triplet (i, j, X) where i is the distance of the beginning of the found prefix from the end of the search buffer, j is the length of the found prefix and X is the first character after the prefix in look-ahead buffer. The following applet visualizes this algorithm. The number of bits written to the output depends on used encoding of numbers.

Ternary Compression:

Suffix encoding is practically the same algorithm as prefix encoding, with the small difference that we use to encode duplicating suffixes.

IV. EXPERIMENTS AND RESULT

Firewall has simple rules such as to allow or deny protocols, ports or IP address. Firewall can effectively prevent users form attacks from machine. Typically, and as shown in Figure 1, The bastion host sits on the internal network. Incoming traffic, from the untrusted network, is forwarded to the bastion host server or firewall that will determine whether or not the messages are forwarded to the trusted network. Outgoing communication can follow the reversed route or can go directly from the trusted to the untrusted network by passing the bastion host. The bastion host thus needs to maintain a high level of host security. The internal networks link the internal servers.

Firewalls are typically deployed at the edge of the network or at the entry point of a private network. Incoming and outgoing Internet traffic is inspected by network firewalls. Based on a set of rules, firewalls can allow or block incoming or outgoing traffic. To accomplish this, network firewalls have a rule-based engine that interrogates incoming packets sequentially rule by rule until a match is found. If an incoming packet matches all conditions of a particular rule, then a certain action is taken, e.g., to pass or drop the packet. A packet can match the conditions of more than one rule. In such a case, the first rule will have priority and its action will be applied to the packet. Accordingly, the firewall checks the rules sequentially, one by one, until a rule is matched.

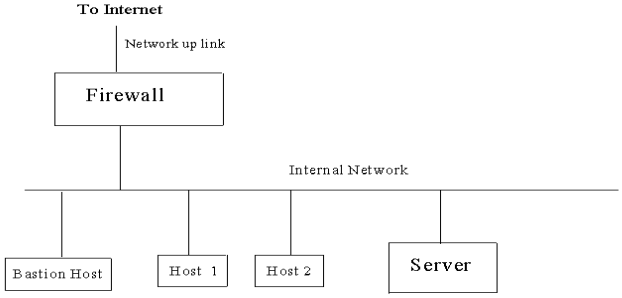

Fig 1. System Architecture

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.2026.0802353

At first we going to capture the network packet transmit over the network. We can capture the network packet using the tool called jpcap After capturing the packet information, we can generate a rule for processing and identify the ddos attack and normal flow attack from captured packet. Incoming and outgoing Internet traffic is inspected by network firewalls. Based on a set of rules, firewalls can allow or block incoming or outgoing traffic.

A. Single or Multiple Flows

We present two models. The first model represents the behavior of a rule-based network firewall when all incoming packets are matched with a single rule at position M. The second model extends the first one to capture the behavior of a firewall when different rule positions are triggered.

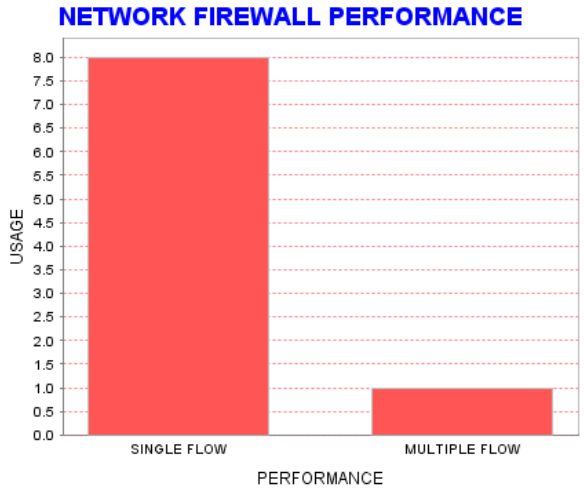

Fig 2. Performance of Single flow and Multiple flow

B. Performance Measures

We report experimental and analysis results of the firewall performance in terms of various key measures which include throughput, packet loss, firewall's CPU utilization, and packet delay. In particular, we report results of these key performance measures when sending a normal traffic and when subjecting the firewall to DoS traffic targeting different rules. In addition, we report analytical results and offer interpretation in order to gain a deeper insight in the firewall dynamics and behavior.We can verify and validate the firewall throughput, packet loss, delay, and CPU utilization.Throughput is the rate at which the computational work is done. CPU utilization is the level of CPU throughput. These measurements were taken when subjecting the firewall to two types of traffic: (1) normal traffic, and (2) DDoS traffic targeting different rules located at different positions in the firewall rulebase.We report results of these key performance measures when sending a normal traffic and when subjecting the firewall to DoS traffic targeting different rules.

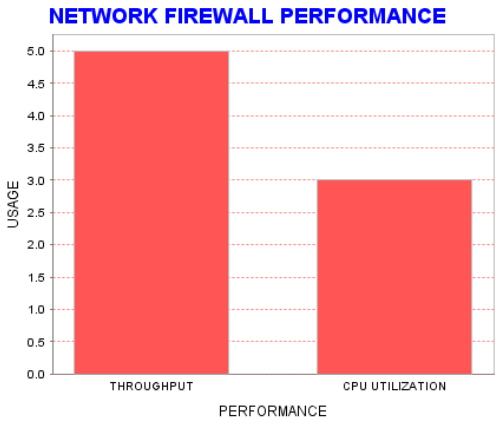

Fig 3 Firewall's throughput and CPU utilization with respect to DOS attack

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

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

DOI:10.15662/IJEETR.2026.0802353

Packet Delay is the variation in the time taken to deliver a series of messages. Packet Loss occurs when one or more packets of data travelling across a network fails to reach their destination.

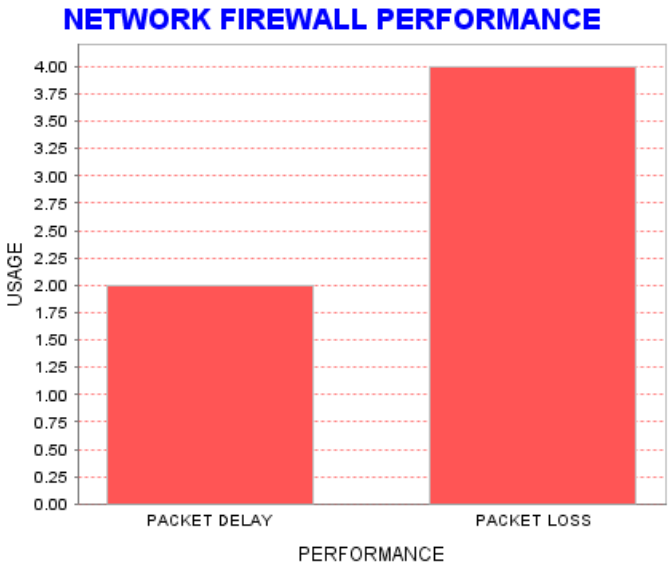

Fig 4. Performance of Packet Delay and Packet Loss

V. CONCLUSION

We have presented and validated an analytical model to study and analyze the performance of rule-based network firewalls. From the model, we have derived key features and performance measures of engineering and design significance. These key features and measures include throughput, packet loss, packet delay, and CPU utilization. The model can be used to measure the performance when the firewall is subjected to normal traffic flows as well as DoS attack flows targeting different rule positions. We identified Dos attack and traffic flow attack in internet server using rule-based firewall and minimized the size of the rule set or rearranged dynamically so that bottom rules can be served at the top of the rule set.

REFERENCES

1. Arbor Networks Inc., "Worldwide infrastructure security report, volume vi," 2010. Available: http://www.arbornetworks.com/report
2. S. Acharya, J. Wang, Z. Ge, T. Znati, and A. Greeberg, "Simulation study of firewalls to aid improved performance," in Proc. 2006 Simulation Symposium.
3. Hickman, D. Newman, S. Tadjudin, and T. Martin, "Benchmarking methodology for firewall performance," RFC3511, Apr. 2003.
4. M. Lyu and L. Lau, "Firewall security: policies, testing and performance evaluation," in Proc. 2000 IEEE International Computer Software and Applications Conference, pp. 116–121.
5. V. Santiraveewan and Y. Permpoontanalarp, "A graph-based methodology for analyzing IP spoofing attack," in Proc. 2004 IEEE International Conference on Advanced Information Networking and Applications, pp. 227–231.
6. S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. Frantzen, "Analysis of vulnerabilities in Internet firewalls," Int'l J. Computers and Security, vol. 22, no. 3, pp. 214–232, 2003.
7. Goldsmith and M. Schiffman, "Firewalking: a traceroute - like analysis of IP packet responses to determine gateway access control lists," Oct. 1998. Available: http://www.packetfactory.net/firewalk/
8. firewalk-final.html
9. 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
10. 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

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

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

DOI:10.15662/IJEETR.2026.0802353

11. K. Salah, K. Sattar, M. Sqalli, and E. Alshaer, "A potential low-rate dos attack against network firewalls," Int'l J. Security and Commun. Networks, vol. 4, no. 2, pp. 109–238, Feb. 2011.
12. S. A. Crosby and D. S. Wallach, "Denial of service via algorithmic complexity attacks," in Proc. 2003 USENIX Security Symposium, pp. 29–44.
13. G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A general framework for benchmarking firewall optimization techniques," IEEE Trans. Network Service Management, vol. 5, no. 4, pp. 227–238, 2008.]
14. Al-Shaer and H. Hamed, "Modeling and management of firewall policies," IEEE Trans. Network Service Management, vol. 1, no. 1, pp. 2–10, 2004.
15. H. Hamed, A. El-Atawy, and E. Al-Shaer, "Adaptive statistical optimization techniques for firewall packet filtering," in Proc. 2006 IEEE INFOCO
16. Al-Shaer and H. Hamed, "Modeling and management of firewall policies," IEEE Trans. Network Service Management, vol. 1, no. 1, pp. 2–10, 2004.
17. L. Yuan, J. Mai, Z. Su, H. Chen, C. Chuah, and P. Mohapatra, "Fireman: a toolkit for firewall modeling and analysis," in Proc. 2006 IEEE Symposium on Security and Privacy.
18. Mayer, A. Wool, and E. Ziskind, "Fang: a firewall analysis engine," in Proc. 2000 IEEE Symposium on Security and Privacy.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.2026.0802353

33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.2026.0802353

53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.
59. 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.
60. 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.
61. 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.
62. 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.
63. 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.
64. 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.
65. 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.
66. 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.
67. 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.
68. 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.
69. 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.
70. 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.
71. 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.
72. 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).
73. 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.2026.0802353

74. 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.
75. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
76. 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.
77. 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.
78. 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).
79. 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.
80. 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.
81. 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.
82. 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.
83. 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.
84. 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.
85. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
86. 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.
87. 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.
88. 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.
89. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
90. 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.
91. 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.
92. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
93. 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.
94. 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.
95. 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.2026.0802353

96. 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.
97. 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.
98. 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.
99. 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).
100. 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.
101. 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.
102. 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.
103. 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.