IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

Threshold Congestion Detection Using Honeypot in DDOS

*R.Udayakumar

Dean- Computer science and IT, Kalinga University, Raipur, CG., India

*deancsit@kalingauniversity.ac.in,rsukumar2007@gmail.com

ABSTRACT: This research paper implements congestion detection using honeypot against DDoS attack. In first level to detect congestion inducing attack. In that large attacks are detected early in the border router in the transit network before converge at server. At the second level to detect the well skilled attacker to reduce the network performance to perform attack with adjustable entropy value that kind of secret attacks are remain undetected in the transit domain. These attacks are detected in the border router in the stub domain near the victim. Honeypot is used to high filtering accuracy. Identified the attacker and deactivate the service for attacker from server. It will help to legitimate user to get frequent service form server. Concept of varying threshold and change point detection on entropy to improve the detection rate. This technique gives high solution to DDoS attack.

KEYWORD: Distributed Denial of Service, Detection, Honeypots, Entropy.

I.INTRODUCTION

The attack detection method is necessary for the DDoS system. The timely detection of DDoS attack, system give proper response to escape big loss .The various techniques have been used for DDoS attack detection [1].Detecting DDoS attack is relatively easy at the victim network [2] because it can observe all the attack packets. However, attack packets clog a large part of the network before they are detected at the victim early attack detection schemes [3] unfortunately have to wait for the flooding to become widespread, consequently, this two level of attack detection performing infiltrating, corruption as well as highly distributed attacks detection.

II. RELATED WORK

Source IP based entropy algorithms are efficient in case of highly distributed DDoS attacks or highly concentrated high bandwidth attacks. A proficient and sophisticated attacker usually tries to defeat the detection algorithm based on source IP based entropy [4] by secretly producing flooding attack and simulating the monitor's expected normal data flow. After knowing some packet attributes' entropy values, these attackers could use the attack tools to produce some flooding with adjustable entropy values. By guess, test or summary these attackers could probably know the normal entropy range in the monitors and adjust their own flooding to match it, although such stealthy attacks are not easy to realize. We improve the previous entropy detection algorithms and propose enhanced algorithms for two level detection. First Level detectors are based on entropy calculated over source IP and second level detectors are based on entropy calculated over destination IP.

2.1 DETECTION FLOW

Detection algorithms are running on the edge routers of transit and stub network. Largest volume of attacks should be detected early and dropped before they enter the victim network. These attack flows that can create congestion in the network and stress resource utilization in a router and network, which make them crucial to be dropped before they enter the network. The detectors on edge routers of transit network consistently detect these attacks and do so with a very low false alarm rate. The edge routers of transit network monitor source IP aggregates. When there is an attack, flows are destined on honeypot and entropy based on source IP aggregates (flows) changes dramatically at router, because there is either one flow dominating the router (this indicates concentrated attack and entropy decreases) or multiple flows with a very few packet arrivals in each flow (this indicates distributed attacks and entropy increases). Second level attacks may not necessarily impact the network, but they can have dramatic impact on the victim or server. Final level detector located on edge routers of stub domain are used for such attacks. They enable highly

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

sensitive detection. System entropy based on destination IP based aggregates (flows) is calculated on edge routers of stub domain for servers to be protected.

2.2 OPTIMUM THRESHOLD AND ENTROPHY

. To measure the entropy using transit-stub network. The entropy is measured by recording dynamic of packet on the border on the two networks. Entropy is used to measure traffic feature distribution .incoming packet entropy range can be detected the entropy range is higher than threshold limit .then transit border router collect information in a time window and calculate system entropy H(X).the H n(X) is a normal entropy. To detect the attack, the entropy Hc(X) is calculated whenever Hn(X) attack is detected. They are using the Honeypot along with the server to detect. Attack is conformed then packets are forward to the Honeypot then Honeypot drop the attack packet. Thus reduce the false negative.

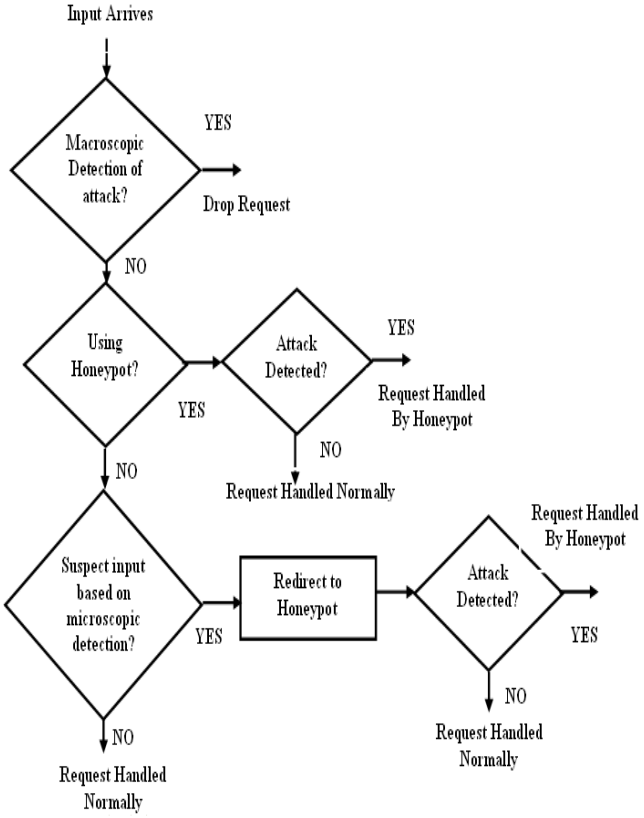

Figure: 1 Detection flow

Attack load can off the server but using Honeypot handle the server to be active to reducing the false positive[6].Fixed threshold to alarm on traffic .if the threshold is set high then false alarm rate will be low but detection rate is low. If threshold set low then detect rate is high but suffer from false alarm is high. This model reflects changes in background traffic. Threshold is depending on network condition .False positive give effectiveness of the system, false negative give the measure of system reliability on optimal value of entropic threshold [7].CUSUM is calculated over destination IP address based entropy to detect the attacks. It makes use of the concept of time along with threshold to judge the network condition. If the abnormal condition persists for a certain period or crosses threshold, attack is detected. Destination under attack is identified in case attack is present. To implement this algorithm, one needs to create database containing large amount of legal IP address. The calculation is complicated and has low efficiency .The destination IP address based entropy statistics. Try to cumulate the entropy according to some rules, thus it will have more accurate DDoS attack detection rate [8]

2.3 SYSTEM SETUP

Transit stub model is based on the hierarchical approach of the Internet [5]. In such a model, every domain can be classified as either a stub network or a transit network. Backbone ISPs and regional ISPs are examples of transit

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

networks. The traffic generating nodes (end hosts) are only connected to Stub networks. Model the Internet to measure the entropy in transit – stub network. During an attack, the Internet or IP domain is divided into the two networks. The entropy is measured by recording the dynamics of packets on the border of the two networks.

	parameter	value
1	Number of legal sources	15-48
2	Number of attackers	1-89
3	Backbone link bandwidth	100 Mbps
4	Bottleneck link bandwidth	10 Mbps
5	Bottleneck link delay	1 msec
6	Access link bw for legitimate clients	1 Mbps
7	Access link delay for legitimate clients	10 msec
8	Server link bandwidth	3 Mbps
9	Server link delay	1 mpbs
10	Mean attacker	rate 0.1-3.0 Mbps (low rate) 3.0 – 6.5 Mbps (moderate rate) > 6.5 Mbps (high rate
11	Mean	load 0.1-7.0 Mbps (low rate) client 7.0-9.0 Mbps (moderate rate) >9.0 Mbps (high rate

TABLE I. BASIC PARAMETERS FOR SIMULATION

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

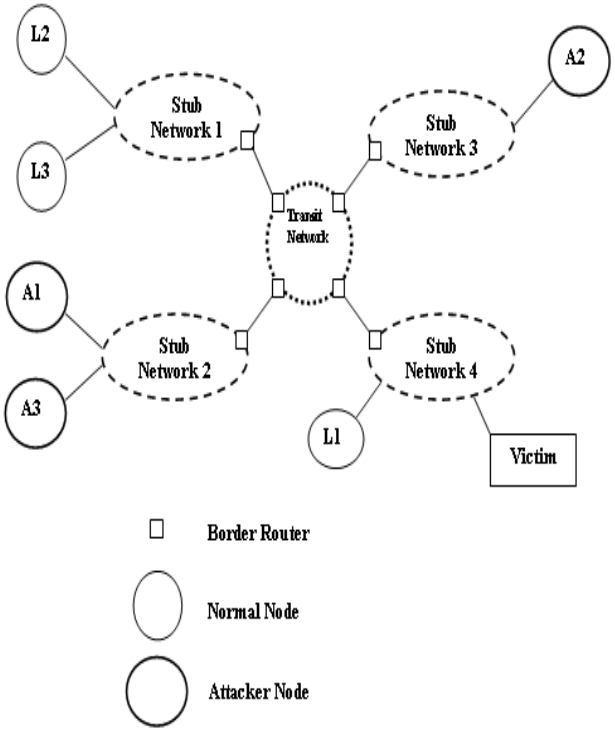

Figure:2 Transit-Stub Network

III. LEVELS OF DDoS ATTACK DETECTION METHOD

Highly distributed DDoS flooding attacks or highly concentrated high bandwidth attacks which induce immediate congestion in the network. They are located on the edge routers of the transit domains and hence enable early DDoS detection without any traffic observation in the victim network. They make use of computing entropies based on source IP addresses and detect an attack if system entropy crosses threshold limits. If the flows are destined to honey pots attack is confirmed and corresponding attack flows are dropped [9]. Final level attack detection are successful in Isolating voluminous congestion inducing attack traffic. Slow rate, isotropic attacks that do not cause immediate congestion may go undetected. Moreover, distributional changes captured by entropy observed on source IP alone cannot detect stealthy and sophisticated attacks that are crafted to match statistics of normal traffic. Discriminate DDoS attacks from surge legitimate accessing is a major challenge. Current volume based detection schemes [9] for attack detection at the victim cannot detect slow rate, isotropic attacks because these attacks do not cause detectable disruptions in traffic volume. A DDoS attack, regardless of its volume and source, will cause the distribution of destination address to be concentrated on the victim address. In DDoS attack scenario, a single destination IP address (or alternatively, a very, very few number of unique destination IP addresses) receives much more traffic than other normal conditions. Hence, observing the time series of entropy on destination IP exposes unusual traffic behavior which source IP alone could not detect. A decline in entropy of the system in the destination IP address based entropy time series indicates Denial of Service attack. using the honeypot to detect the attacker and deactivate the attacker service from server. It will help to legitimate user to get frequent service form server.

Final attack detectors designate different flow IDs to each unique Destination, DestinationPort encountered in incoming packet. In other words, we define flow as the packets that share same destination address at the edge router of stub network. Our attack detection algorithm is based on the Sequential Change Point Detection.In the non parameter CUSUM algorithm, the idea of sequential variation is proposed . To implement that algorithm, one needs to create database containing large amount of legal IP address. The calculation is complicated and has low efficiency. In our improvement, we use the destination IP address based entropy statistics. The advantage of this improved algorithm is that it comprises implicitly a concept of process cumulating. The function of cumulating process is to avoid false alarm whe the network has something abnormal just at a time point like a surge of legitimate access. Thus the threshold based approach leads to a more real time attack detection. Time based approach emphasizes on time tolerance and ignores network anomalies in some allowable range.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

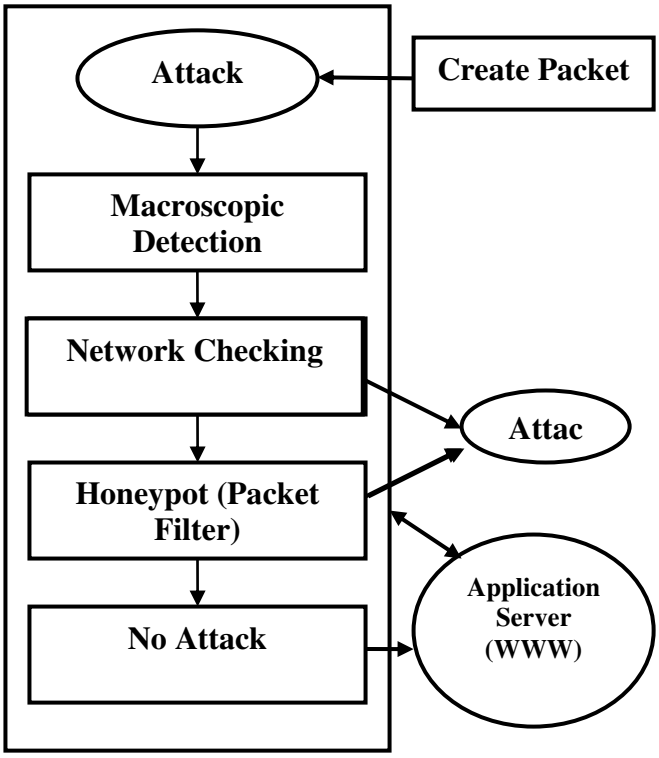

Figure: 3 System Design

IV.IMPLEMENTATION

The above design is proposed to be implemented using NS2 (network simulator2) and results obtained shall be tabulated and analyzed for further enhancement.

V.CONCLUSION

This method used for detecting a large variety of DDoS attacks. It detects congestion inducing attacks at the early stage, without any collateral damage. Stealthy and sophisticated attacks that remain undetected are detected near the victim. Even very meek rate DDoS attacks are detected reliably early in the network. The results show that honeypots have the potential to suppress false alarms and false negatives, thus improving the detection rate. To calculate optimum entropic thresholds for varying attack loads in real time to self-calibrate the system promises accurate real time attack detection. The simulation experiments yielded very high detection rates.

REFERENCES

[1] Kalaiprasath, R; Elankavi, R; Udayakumar, R; , Cloud security and compliance-a semantic approach in end to end security, International Journal on Smart Sensing and Intelligent Systems, V-10, I-5, PP:482-494, 2017.

[2] Elankavi, R; Kalaiprasath, R; Udayakumar, R; , Wireless Zigbee Network Cluster-Capacity Calculation and Secure Data Conveyance Using Indegree, International Journal on Smart Sensing and Intelligent Systems, V-10, I-5, PP:174-185, 2017.

[3] Kalaiprasath, R; Elankavi, R; Udayakumar, R; , A New Approach for Cloud Data Security: From Single to Cloud-of-Clouds, International Journal on Smart Sensing and Intelligent Systems, V-10, I-5, PP:604-613, 2017.

[4] Elankavi, R; Kalaiprasath, R; Udayakumar, R; , Data Mining with Big Data Revolution Hybrid, International Journal on Smart Sensing and Intelligent Systems, V-10, I-5, PP:560-573, 2017.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

[5] Elankavi, R; Kalaiprasath, R; Udayakumar, Dr R; , A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), V-8, I-5, PP:1220-1227, 2017.

[6] Gajmal, Yogesh M; Udayakumar, R; , Blockchain-based access control and data sharing mechanism in cloud decentralized storage system, Journal of web engineering, PP:1359–1388-1359–1388, 2021.

[7] Gajmal, Yogesh M; Udayakumar, R; , A Bibliometric Analysis of Authentication based Access Control in Cloud using Blockchain, Library Philosophy and Practice, PP:0_1-16, 2021.

[8] Shirke, S; Udayakumar, R; , Robust lane identification by using EW-CSA based DCNN, J. of Critical Reviews, V-6, PP:18-21, 2019.

[9] Subhash, Ligade Sunil; Udayakumar, R; , A BIG SHARK ADAPTION ALGORITHM BASED RESOURCE ALLOTMENT APPROACH IN CLOUD COMPUTING ENVIRONMENT, PalArch's Journal of Archaeology of Egypt/Egyptology, V-17, I-7, PP:5374-5379, 2020.

[10] Gajmal, Yogesh M; Udayakumar, R; , Privacy and utility-assisted data protection strategy for secure data sharing and retrieval in cloud system, Information Security Journal: A Global Perspective, V-31, I-4, PP:451-465, 2022.

[11] Gajmal, Yogesh M; Udayakumar, R; , Analysis of Authentication based Data Access Control Systems in Cloud, PalArch's Journal of Archaeology of Egypt/Egyptology, V-17, I-7, PP:5319-5328, 2020.

[12] Shirke, Suvarna; Udayakumar, R; , Evaluation of crow search algorithm (CSA) for optimization in discrete applications, 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), PP:584-589, 2019.

[13] Shirke, Suvarna; Udayakumar, Ramanathan; , A novel region-based iterative seed method for the detection of multiple lanes, International Journal of Image and Data Fusion, V-11, I-1, PP:57-76, 2020.

[14] Shirke, Suvarna; Udayakumar, R; , Fusion model based on entropy by using optimized DCNN and iterative seed for multilane detection, Evolutionary Intelligence, PP:44940, 2022.

[15] Shirke, Suvarna; Udayakumar, R; , Hybrid optimisation dependent deep belief network for lane detection, Journal of Experimental & Theoretical Artificial Intelligence, V-34, I-2, PP:175-187, 2022.

[16] Subhash, Ligade Sunil; Udayakumar, R; , Sunflower whale optimization algorithm for resource allocation strategy in cloud computing platform, Wireless Personal Communications, V-116, PP:3061-3080, 2021.

[17] Subhash, Ligade Sunil; Udayakumar, R; , A Supremacy–Responsive Resource Distribution Technique for Controlled Workflow Implementation in Cloud Surroundings, Solid State Technology, V-63, I-5, PP:7662-7669, 2020.

[18] Sindhu, Velagapudi Swapna; Lakshmi, Kavuri Jaya; Tangellamudi, Ameya Sanjanita; Lakshmi, C; , A Deep Learning Approach For Detecting Type 2 Diabetes Mellitus, 2022 International Conference on Computer Communication and Informatics (ICCCI), PP:44936, 2022.

[19] Priyan, Siluvayan; Udayakumar, R; Mala, Pitchaikani; Prabha, Mariappan; Ghosh, Ananya; , A sustainable dual-channel inventory model with trapezoidal fuzzy demand and energy consumption, Cleaner Engineering and Technology, V-6, PP:100400, 2022.

[20] Elankavi, R; Kalaiprasath, R; Udayakumar, R; , Potential Exploitation of Broadcasting System Using Multiple Smart Directional Antennas-Help of Sensor Network, International Journal of Mechanical Engineering and Technology (IJMET), V-8, I-6, PP:678-687, 2017.

[21] Udayakumar, R; Kalam, Muhammad Abul; , Sentiment Analysis Using Machine Learning Algorithms,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

Mathematical Statistician and Engineering Applications, V-71, I-3s2, PP:1186–1200-1186–1200, 2022.

[22] GAJMAL, YOGESH M; UDAYAKUMAR, R; , Data Access Controls in Cloud: A Survey., International Journal of Pharmaceutical Research (09752366), V-12, I-4, 2020.

[23] Udayakumar, R; Khanaa, V; Kaliyamurthie, KP; , Optical ring architecture performance evaluation using ordinary receiver, Indian Journal of Science and Technology, V-6, I-6, PP:4742-4747, 2013.

[24] Udayakumar, R; Khanaa, V; Kaliyamurthie, KP; , Performance analysis of resilient ftth architecture with protection mechanism, Indian Journal of Science and Technology, V-6, I-6, PP:4737-4741, 2013.

[25] Udayakumar, R; Khanaa, V; Saravanan, T; , Synthesis and structural characterization of thin films of sno2 prepared by spray pyrolysis technique, Indian Journal of Science and Technology, V-6, I-S6, PP:4754-7, 2013.

[26] Udayakumar, R; Khanaa, V; , Health monitoring system for induction motors, Int. J. Eng. Comput. Sci, V-2, I-4, PP:1117-1122, 2013.

[27] Udayakumar, R; Khanaa, V; , Quantum Computers-A Revolution InComputing, Quantum, V-8, I-4, PP:33-36, 2013.

[28] Khanaa, V; Udayakumar, R; , Protecting privacy when disclosing information: k anonymity and its enforcement through suppression, database, V-1, I-2, 2012.

[29] Khanaa, V; Udayakumar, R; , Hybrid Fuzzy Approches for Networks, International Journal of Innovative Research in science, Engineering and Technology, V-12, I-3, PP:24-31, 2012.

[30] Udayakumar, R; Khanaa, V; Saravanan, T; Saritha, G; , Cross layer optimization for wireless network (WIMAX), Middle-East Journal of Scientific Research, V-16, I-12, PP:2013, 2012.

[31] Udayakumar, R; Thooyamani, KP; Khanaa, V; , Coarse-Grained Parallel Genetical Gorithm to Solve the Shortest Path Routing Problem Using Genetic Operators, Middle-East Journal of Scientific Research, V-15, I-12, PP:1651-1654, 2013.

[32] Khanaa, V; Udayakumar, R; , Efficient Pc Controlled By Hand Movement Using Mems Sensor Mouse, Indian Journal of science and Technology, V-12, I-6, PP:1438-1442, 2012.

[33] Udayakumar, R; Khanaa, V; , Sixth Sense Technology, International Journal Of Engineering And Computer Science, V-2, I-4, 2013.

[34] Udayakumar, R; Thooyamani, KP; Khanaa, V; , Secure Incentive Protocol for Multi-Hop Wireless Network with Limited Use of Public Key Cryptography, Middle-East Journal of Scientific Research, V-20, I-11, PP:1651-1656, 2014.

[35] Udayakumar, R; Kaliyamurthie, KP; Khanaa, TK; , Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, V-29, I-14, PP:86-90, 2014.

[36] Udayakumar, R; Saravanan, T; , Tailored Image District Processing Precision Andwritten Appreciation, Middle-East Journal of Scientific Research, V-20, I-11, PP:1615-1625, 2014.

[37] Udayakumar, R; Thooyamani, KP; , Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, V-29, I-14, 2014.

[38] Udayakumar, R; Thooyamani, KP; , Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, V-29, I-1, PP:24-31, 2014.

[39] Thooyamani, KP; Khanaa, V; Udayakumar, R; , Wide area wireless networks-IETF, Middle-East Journal of Scientific Research, V-20, I-12, PP:2042-2046, 2014.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104283 |

[40] Khanaa, V; Thooyamani, KP; Udayakumar, R; , Modelling Cloud Storage, World Applied Sciences Journal, V-29, 2014.

[41] Khanaa, V; Thooyamani, KP; Udayakumar, R; , Elliptic curve cryptography using in multicast network, World Applied Sciences Journal, V-29, 2014.

[42] Khanaa, V; Thooyamani, KP; Udayakumar, R; , Two factor authentication using mobile phones, World Applied Sciences Journal, V-29, I-14, PP:208-213, 2014.

[43] Khanaa, V; Thooyamani, KP; Udayakumar, R; , Patient monitoring in gene ontology with words computing using SOM, World Applied Sciences Journal, V-29, 2014.

[44] Kaliyamurthie, KP; Parameswari, D; Udayakumar, R; , Malicious packet loss during routing misbehavior-identification, Middle-East Journal of Scientific Research, V-20, I-11, PP:1413-1416, 2014.

[45] Udayakumar, R; Saritha, G; Saravanan, T; , Modelling and Simulation of Electromechanical Systems Working with Nonlinear Frictional Loads and Controlled by Subordinated Control System of Coordinates, Middle-East Journal of Scientific Research, V-20, I-12, PP:1918-1923, 2014.

[46] Saravanan, T; Saritha, G; Udayakumar, R; , Cassette Steganography for Entrenched Metaphors in Squashed Videos, Middle-East Journal of Scientific Research, V-20, I-12, PP:2475-2478, 2014.

[47] Udayakumar, R; Khanaa, V; Saravanan, T; , Energy Demand Management Motor Control Using Multilevel Inverter, Middle-East Journal of Scientific Research, V-20, I-12, PP:2613-2619, 2014.

[48] Thooyamani, KP; Khanaa, V; Udayakumar, R; , Wireless cellular communication using 100 nanometers spintronics device based VLSI, Middle-East Journal of Scientific Research, V-20, I-12, PP:2037-2041, 2014.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details