Application Layer DDoS Attack Defense Methods with a New Method against Flooding

Sreeja Nair M. P., Mathew Cherian, Preetha Mathew K.

Abstract: ***In a network environment, Distributed Denial of Service (DDoS) attacks eemploys a network or server is unavailable to its normal users. Application-layer Distributed Denial of Service (App-DDoS) attacks are serious issues for the webserver itself. The multitude and variety of such attacks and defense approaches are overwhelming. This paper here follows, we analyze the different defense mechanisms for application-layer DDoS attacks and proposes a new approach to defend using machine learning.***

Keywords: Application Layer-DDOS Attacks, Defense

I. INTRODUCTION

Distributed Denial of Service (DDoS) attack is a coordinated mass-scale attack on the availability of services of a network with many compromised computing systems. The victims of DDoS attacks are mostly on the systems of giant corporate organizations and governments of various states. According to Verisign, DDoS activity hampered the pace of the Internet by 85% in the last two years with 32% of those attacks targeting software-as-service, IT services, and computing firms in 2015.

A. Different DDoS attacks on Application Layer

SLOW READ DDoS attack involves an attacker sending an appropriate HTTP request to a server, but reads the response at a very slow speed causing slow traffic.
SLOWPOST DDoS attacker sends legitimate HTTP POST headers to a web server with correctly specified sizes of the message body. However, the message body is sent at a low speed, such as one byte in two minutes. When the attacker sends such SLOW POST in large numbers at the same time, server resources are rapidly consumed, making legitimate connections unachievable.
SLOW LORIS ATTACK uses partial HTTP requests to open connections to target webserver and slows down the system
By keeping it open as long as possible. This type of attack requires minimal bandwidth to launch and impacts the target web server leaving other services and ports unaffected.
HTTP PRAGMA ATTACK uses PRAGMA, the header field intended for HTTP protocol requests, for an indefinite time blocking the socket resources.

Revised Manuscript Received on February 15, 2020.

*** Sreeja Nair M. P.,** Faculty and Research Scholar, Cochin University College of Engineering Kuttanad, Cochin University of Science and Technology, Kerala, India. Email:sreejanairmp@gmail.com

Dr. Mathew Cherian, Department of Mechanical Engineering, Cochin University College of Engineering Kuttanad, Cochin University of Science and Technology, Kerala, India. Email:mathewch1@gmail.com

Dr. Preetha Mathew K., Faculty and Research Scholar, Cochin University College of Engineering Kuttanad, Cochin University of Science and Technology, Kerala, India.Email:preetha.mathew.k@gmail.com

HTTP FLOODING ATTACK, floods the target web application with huge URL requests. It may be HTTP GET attack or HTTP POST attack.
DNS PROTOCOL ATTACK subdues the DNS server with large number of queries making ineffective in handling online queries further after a period of time and forces to go offline.
SQL INJECTION ATTACK renders the system ineffective in executing SQL statements by injecting spurious SQL lines.
XML INJECTION Attacker inserts malicious statements into the XML causing to consume server excessive memory the various attacks known are listed in Table.1.

Table.1. Application layer DDoS attacks with its features

Attack	Features
Slow Read	Fast read but slow response by the server
Slow Post	Large amount of slow post Requests at the same time
Slow Loris	HTTP connections are open always by sending it partially
HTTP PRAGMA	Indefinitely blocking the resources
HTTP flooding	Flood the target with huge number of requests
DNS Protocol	Down the DNS Server
SQL Injection	Inserting malicious codes to SQL Queries

II. APPLICATION LAYER DDOS DEFENSE METHODS

Usual Defense Techniques for DDoS attacks are listed: [1]

1) *Disabling Unused Services* involves reducing the number of open ports and applications to a minimum, lessening the vulnerability to such attacks. Examples of such attacks are User Datagram Protocol (UDP) echo packets and character services.
2) *Installing Latest Security Patches* allows the system to update usually and avoids it from the exploitation of vulnerabilities
3) *Disabling IP Broadcast thwarts* ICMP flood and smurf attacks
4) *Maintaining Firewall* chokes unauthorized users by simply regulating IP features.
5) *Global Defense Infrastructure* filters router from attacks.
6) *IP Hopping* restricts DDOS attack by rearranging the locator or IP address of the server from a group of servers or a pre-arranged set of IP addresses. But such a process can also make the system vulnerable.

Various Filtering Techniques [2] employed to counter DDoS attacks are as follows

Ingress/Egress Techniques are input/output-based filtering. While the Ingress filtering technique restricts all inbound spoofed IP addresses which are incoherent with Domain address, Egress filtering technique allows packets to leave router after assigned and allocated IP addresses. However, such input/output filtering can block legitimate packets when their routes are changed and are spurious to asymmetric and dynamic Routing.

History-Based IP Filtering [2] such as Hash or Bloom filtering techniques, blocks those IP addresses marked as spam or thrash. However, those DDoS attacks from "new" spurious IP address cannot be recognized by such Filters.

Secure Overlay Service (SOS) defines secure interaction in the architecture itself that guarantees safe communication between legitimate users and the target system.

Source Address Validity Enforcement (SAVE) protocol filter packets from spoofed source addresses while allowing from the expected source which is constantly updated.

Table.2.General Techniques for Application Layer DDoS Attacks

Technique Name	Features
Disabling Unused Services	Reducing the number of open ports and applications to a minimum
Installing Latest Security Patches	Update the system regularly
Ingress/Egress	Filter incoming or outgoing IP addresses
History-Based IP Filtering	Filter IP addresses based on history
Secure Overlay Service (SOS)	Secure interaction architecture developed
Source Address Validity Enforcement (SAVE) Protocol	Filter spoofed source addresses

Application-based techniques for defending against DDoS [1] are also prevalent:

Defense against Tilt (DAT) [3] monitor features namely sudden traffic, volume, session characteristics etc. for countering DDoS .*Hybrid/Distributed mechanisms* provides collaboration and connection between clients and server to identify and respond to DDoS attacks. The *Speak-Up* [4] mechanism is employed to counter session flooding attacks by differentiating the good and bad clients based on characteristics of the server's resources. *DOW (Defense and Offense Wall)* mechanism [5] uses the K-Means clustering method to identify, filter session and flooding as well as asymmetric attacks. *Bot flooding prevention* [6] mechanisms differentiate legal users and spurious non-human users (bots) vide Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA). *Admission and Congestion Control* limits the number of concurrent clients via port hiding and online services rendering. *Trust Management Helmet (TMH)* [8] protects the connectivity of authentic users from illegitimate and attackers. Hybrid detection mechanism based on trust and information metrics filters out suspicious flows based on its trust value, information and user browsing behaviour such as HTTP Request rate, page viewing time, etc.

Table.3. Application bases techniques to defend application layer DDoS

Technique Name	Features
Defense against Tilt (DAT)	monitor features like IP characteristics.
Speak-Up	differentiating the good and bad clients based on characteristics of server's resources.
DOW (Defense and Offense Wall)	K-Means clustering
Bot flooding prevention	CAPTCHA Technique
Admission and Congestion Control	limits the number of clients based on port and online services
Trust Management Helmet (TMH)	connectivity of authentic users

To protect servers from attack, Supranamaya et al [2] introduced a degradation-mechanism, namely "DDoS Shield". It has two components, suspicion assignment mechanism, and DDoS-resilient scheduler. The suspicion mechanism assigns suspicion measure value-based history session history to each client. The Scheduler on the other hand, utilizes the values to determine the scheduling of session's requests using testbed experiments based on certain scheduling policies that estimate the potency of attacks on web applications for choosing efficient counter-mechanism. *Lowest Suspicion First (LSF)* Scheduler is based on optimization of cost such that for N sessions at any time with suspicion metric p_i and average response time *Ti* realizes an Objective Function $\min \sum_{i=1}^{N}(1-pi)/Ti$. Intuitively, this objective function maximizes the sum of suspicion values *pi* of requests queued at the DDoS scheduler so that those with low suspicion are forwarded to web cluster.

To block automated requests, Suriadi et al. [18] proposed computation-bound hash-based puzzles, but are vulnerable to the sophisticated attacks using image processing algorithms [10] – [11]. Recently, Praseed and Thilagam [9] proposed a user puzzle that can be resolved by human users, but comparatively difficult to complete systems. Examples of the user puzzles are CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) and AYAHs (Are You A Human). It restricts, to a large extent, the DDoS attack from automated requests using botnets or small DDoS tools or script tags available on the Internet and allows human requests alone to be delivered to webserver. However, user puzzles can burden users in solving them, thus reducing the web experience. Another method to block automated requests uses a detection method to detect them and block it. Different types of detection methods are namely: Template matching of individual requests is done by tracking, by analyzing the request stream dynamics and semantics etc.[9].They also proposed defense methods against the ***Asymmetric DDoS Attacks*** that blocks many raising of red flags and other warning signals for detection.

Jensen et al. [12] proposed ***an XML DDoS Defense technique*** by strengthening the schema of Web service in XML query through stricter validation of structure of incoming message in Web Service Description Language (WSDL) as well as hardening by imposing further restrictions on input message fields.

To prevent DNS DDoS Attack, Pappas[13] proposed to increase cache to store infrastructure reports more so that already checked and allowed addresses are not further processed for DDoS attack detection and thus reducing efforts by focusing on new incoming packets only. On the other hand, Zhu et al. [14] suggested enhanced privacy and security by negotiating for alternate connections at the DNS communication level using Transport Layer Security (TLS) protocol. However, it allows to establish connection-oriented attacks like HTTP attacks. Hussain and Abdesselam [16] focus on ***Session Initiation Protocol attack*** (SIP DDoS Attack) and maintaining an intermediate Register server in voice interaction environment that registers the identity of caller and Calle beforehand, assigns each interaction with Critical Number (CN) and filtering as per Session Initiation Protocol (SIP) to the Calle only. But the DDoS attacks from Calle is not handled here and is addressed by Chen [15] by proposing a finite state machine maintains the SIP state. Ideally, this is cost-effective when deployed at client side.

In ***DNS amplification attacks***, the DDoS attacker generates responses by simple queries from several "innocent" servers and directs to victim server causing flooding and chocking. Kambourakis et al. [17] suggested a scheme to identify the "orphan" responses (without query from victim server) under the suspicious category for further verification and rejection of spurious responses. The bloom filter introduced by Sun et al. [19] raises the flag when incoming the responses do not tally with corresponding outgoing requests. Khan et al. [20] experimented chaos theory to detect whether the incoming DNS stream as malicious or not by comparing with past history of streams.

Ndibwile and Govardhan [19] conceptualized a a customized intrusion prevention system in the network layer gateway with a series of three servers: Real, Bait and Decoy Web servers, uses rules generated by an algorithm called random tree machine learning using Snort Network Intrusion Prevention System (NIPS) signatures in supervised learning environment for ***mitigating undetected and malicious traffic*** that intrudes as well as mimics legitimate. While Bait web server uses the same IP address as well as exposure to the public as the Real web server, it receives, segregates and sends illegitimate traffic to Decoy web server where it is registered for future detection of DDoS attacks.

The method proposed by Tetsuya et al. [20] in **d*efense of the large-scale distributed Slow HTTP DDoS attack*** consists of three steps, namely: detection of the presence of DDoS attack via monitoring duration time of connections, extracting source IP addresses connected beyond allotted duration and lastly, disconnecting them. As for the defending Slow HTTP DDoS attacks, Dantas and Nigam [21] employed Adaptive Selective Verification (ASV) mechanism used to countermeasure DDoS Attack to Network Layer into Application Layer Adaptive Selective Verification (ASV) mechanism used to countermeasure DDoS Attack to Network Layer into Application Layer also by stimulating possible attacks such as HTTP PRAGMA ATTACK, GET FLOOD ATTACK, HTTP POST ATTACK based on past transaction details. On the other hand, Hong and Kim [22] envisages such DDoS attacks on server based on whether the number of incomplete HTTP requests or open connections exceeds pre-determined threshold value and then for detailed check on genuineness of the incoming packets for further processing as to accept or discard.

Wang, et al., [24] suggested "sky shield" or Sketch-Based system to defend **Application Layer DDoS Attacks** by comparing the sketch or structure of spurious packets from past DDoS attacks as to determine **whether current/incoming is to be categorized as spurious.** To extract malicious hosts, they use a concept of Hellinger distance which calculate the divergence between sketches for two consecutive cycles.

Stevanovic and Vlajic [25] suggested a method **in *Dynamic Web-Domains*** which uses a drift value based on data mining theory and their variants.

Defending HTTP floods attack at the Application Layer is achieved by incorporating Firewalls at this level or enabling Application layer software with the Defense Mechanisms to detect deviations in dynamics or semantics of request streams to distinguish an attacking situation from normal. *Analysis of dynamics* focusses on one hand on *the modelling of traffic of the request rate* to detect significant deviation from expected value estimated from historical data (Ni et al.[28]) and on the other hand by *the interpretation of analysis outcomes of statistical features* to differentiate HTTP floods attack from the normal streams [26]-[27]. A plethora of schema with different combination of analysis methods over the various features are proposed by different researchers. Deviations of semantics of the request streams are estimated based on its composition or sequence. However, in Defense Mechanisms based on the *analysis of Semantics, the Request streams are graded* as malicious floods attack or legitimate by evaluating parameters generated by the Request stream based on its workload profile in the case of Request composition strategy and features based on the processing requirements in the case of Request Sequence strategy

Table.4. Proposed Application layer DDOS Defense methods by Researchers

Proposed	By whom	attack	Advantages
DDoS Shield	Supranamaya Ranjan	Session Hijacking	Different Scheduling policies
User puzzles like CAPTCHA	Suriadi et al.,	Automated requests	Identifies bot or human
Hardening and validation	Jensen et al	XML DDoS	Restricting messages in the input field
Increase cache	Pappas	DNS DDoS Attack	Already checked and allowed addresses are not further processed
Intermediate Register server	Hussain and Abdesselam	SIP Attack	Assigns Critical Number (CN) and filtering
Chaos theory	Khan et al	DNS amplification attacks	comparing with past history of streams
ASV	Dantas and Nigam	Slow HTTP DDoS attack	Discard if open connections exceed pre-determined threshold values

the modelling of traffic request rate	Wen, et al., Ni et al.	HTTP floods attack	Distinguish an attacking situation from normal situation

III. A NEW DEFENSE APPROACH FOR APPLICATION LAYER DDOS ATTACK

We propose a level-based algorithm to ease HTTP flooding attacks by progressively filtering malicious requests at each level to build more robustness in defending DDOS attacks.

Algorithm

1.CAPTCHA TEST
2.APPLY RTB RULE
3.APPLY DECISION TREE MACHINE LEARNING RULE FOR TRAINING OR PROCESSING REQUESTS
4.SEND ACKNOWLEDGEMENTS

Initially, CAPTCHA TEST is employed to filter out the non-human requests such as bot. In next level, the communication parameters exceeding pre-fixed threshold values are filtered. In third are compared with pre-fixed threshold values to filter request processing parameters. The first phase is not only a solution to avoid DDoS Attacks because the requests are coming from a single user or a multiple connection environment. Here an important factor to be noted is what type of requests are sent by the clients whether they are malicious, overwhelmed or not. So, we need to use second level security. We focus this issue in the second step and try to provide the next level of security. In the second step, first we need to form a reservoir and store the incoming packets. Then analyze the requests from clients by applying a rule named RTB in which we are taking communication parameters with critical comparison. If the comparison result is positive, stops the clients for communication process. Otherwise client requests are taken for further processing and stores them into a buffer. But in this phase also we are not able to confirm the requests are genuine or not since IP spoofing, password cracking, dumpster diving, sniffing, masquerade, replay attack or man in the middle attack may happen in this session. To address this problem, in the last step, we can do an accurate matching technique that performs the identification of genuine Addresses. Here we suggest a machine learning algorithm approach with decision tree by supervised learning to classify the requests and checks their matching. Appropriate matches show the genuine of the client requests and block others. So, we can extract legitimate clients from the buffer more accurately. Then send their acknowledgments.

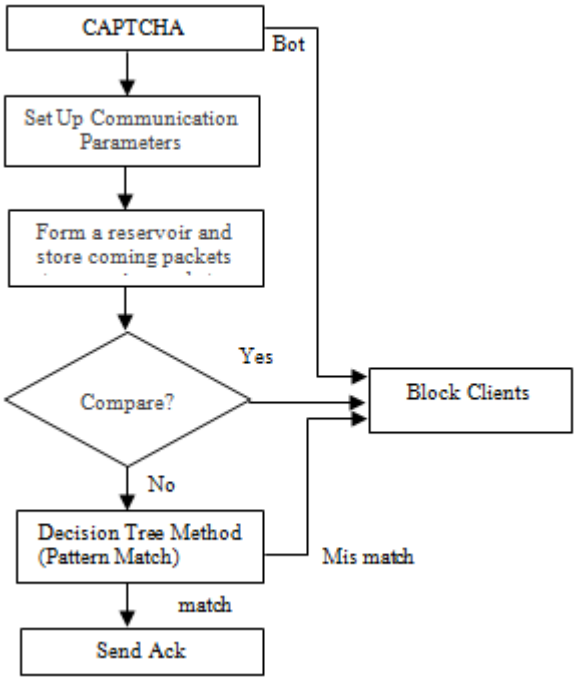

Fig.1.1 Flow of new approach

IV. RESULT AND DISCUSSION

Our paper introducing a new idea with decision tree machine learning. It provides a three layer security with minimum cost. The following table shows the advantages of our proposed idea.

Table.5. Advantages of Proposed Application layer DDOS Defense method

Parameters	Existing System	Proposed System
Bandwidth	Not set previously	Set up as a threshold
Server utilization	low	High
Congestion	May be	Not formulate
hijacking	Less effective	More Effective
Authenticity	minimum	maximum
Flooding	more	less
Injection of malicious data	more	less

V. CONCLUSION

An outlook of defense mechanisms against DDoS attack we have seen there are so many defense mechanisms evolved. But they are failing to face 100% effectiveness in a system. Some mechanisms have low complexity and some of them are limited to do one quality.

In our proposed algorithm it gives three-layer security. So, effectiveness increased by 95%. Availability and scalability are increased. Exact differentiation is possible.

ACKNOWLEDGEMENT

Sincere Thanks to all who gave support and confidence for this work.

REFERENCES

1. Karuna S. Bhosale, Maria Nenova, Georgi Iliev, "The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer", TELKIS 2017.
2. Supranamaya Ranjan, Mustafa Uysal, Edward Knightly, "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 17, NO. 1, FEBRUARY 2009S.Bhosale,et al. "The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms in Application Layer", TELKIS 2017.
3. HI Liu, KC Chang, "Defending systems Against Tilt DDoS attacks", Telecommunication Systems, Services, and Applications (TSSA), pp.22-27, October 20-21, 2011
4. Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger , and Scott Shenker," DDoS Defense by Offense", SIGCOMM '06, September 11–15, 2006
5. Jie Yu, Zhoujun Li, Huowang Chen, Xiaoming Chen, "A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks", Liu et al. "Defending systems Against Tilt DDoS attacks", Telecommunication Systems, Services, and Applications (TSSA), pp.22-27, October 20-21, 2011
6. S Kandula, D Katabi, M Jacob, A Berger, "Botz-4-sale: surviving organized ddos attacks that mimic flash crowds", Proc. of Symposium on Networked Systems Design and Implementation (NSDI), Boston, May 2005.
7. Mudhakar Srivatsa, Aun Iyengar, and Jian Yin, "Mitigating Application-Level Denial of Service Attacks on Web Servers: A Client-Transparent Approach" ACM Transactions on the Web, Vol. 2, No. 3, Article 15, Publication date: July 2008.
8. Jie Yu, Chengfang Fang†, Liming Lu, Zhoujun Li, "A Lightweight mechanism to Mitigate Application Layer DDoS Attacks", Proc. Of Info scale 2009, LNICST 18, pp. 175191, 2009
9. Amit Praseed and P. Santhi Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019.
10. Mori and J. Malik, "Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA," in Proc. IEEE Comput. Soc. Conf.Comput. Vis. Pattern Recognit., vol. 1. Madison, WI, USA, 2003, pp. I–I.
11. J. Yan and A. S. E Ahmad, "Breaking visual CAPTCHAs with naive pattern recognition algorithms," in Proc. IEEE 23rd Annu.Comput. Security Appl. Conf. (ACSAC), Miami Beach, FL, USA, 2007, pp. 279–291.
12. M. Jensen, N. Gruschka, and R. Herkenhöner, "A survey of attacks on Web services," Comput. Sci. Res. Develop., vol. 24, no. 4, pp. 185–197,2009.
13. V. Pappas, D. Massey, and L. Zhang, "Enhancing DNS resilience against denial of service attacks," in Proc. 37th Annu. IEEE/IFIP Int.Conf. Depend. Syst. Netw. (DSN), Edinburgh, U.K., 2007, pp. 450–459.
14. L. Zhu et al. "T-DNS: Connection-oriented DNS to improve privacy and security (poster abstract)," ACM SIGCOMM Comput. Commun.Rev., vol. 44, no. 4, pp. 379–380, 2015.
15. E. Y. Chen, "Detecting DoS attacks on SIP systems," in Proc. 1st IEEE Workshop VoIP Manag. Security, Vancouver, BC, Canada, 2006, pp. 53–58
16. I.Hussain and F. Naït-Abdesselam, "Strategy based proxy to secure user agent from flooding attack in SIP," in Proc. 7th IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Istanbul, Turkey, 2011, pp. 430–435.
17. G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS amplification attacks," in Proc. Int. Workshop Crit.Inf. Infrastruct. Security, 2007, pp. 185–196.
18. S. Suriadi, D. Stebila, A. Clark, and H. Liu, "Defending Web services against denial of service attacks using client puzzles," in Proc.IEEE Int. Conf. Web Services (ICWS), Washington, DC, USA, 2011, pp. 25–32
19. Jema David Ndibwile, A. Govardhan, Kazuya Okada, Youki Kadobayashi, "Web Server Protection against Application Layer DDoS Attacks using Machine Learning and Traffic Authentication", 2015 IEEE 39th Annual International Computers, Software & Applications Conference
20. Tetsuya Hirakawa, Kanayo Ogura, Bhed Bahadur Bista, Toyoo Takata, "A Defense Method against Distributed Slow HTTP DoS Attack", 2016 19th International Conference on Network-Based Information Systems .
21. Yuri G Dantas, Vivek Nigam, Iguatemi E Fonseca, "A selective Defense for Application Layer Attack",2014 IEEE Joint Intelligence and Security Informatics Conference.
22. Kiwon Hong, Youngjun Kim, Hyungoo Choi, Jinwoo Park, "SDN-Assisted Slow HTTP DDoS Attack Defense Method", IEEE COMMUNICATIONS LETTERS Vol.22, N0.4, April
23. Jennifer Steve, "Types of DDoS Attack and their prevention and mitigation strategy", EC-council 2018
24. Wang et al. "Sky Shield: A Sketch-Based Defense System Against Application Layer DDoS Attacks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 3, MARCH 2018
25. Dusan Stevanovic and Natalija Vlajic, "Application-Layer DDoS in Dynamic Web-Domains: Building Defenses against Next-Generation Attack Behavior".
26. K. J. Singh, K. Thongam, and T. De, "Entropy-based application layer DDoS attack detection using artificial neural networks," Entropy, vol. 18, no. 10, p. 350, 2016.
27. K. J. Singh and T. De, "MLP-GA based algorithm to detect application-layer DDoS attack," J. Inf. Security Appl., vol. 36, pp. 145–153, Oct. 2017.
28. T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer DDoS attack using time series analysis," J. Control Sci. Eng., vol. 2013, p. 4, Aug. 2013.

AUTHORS PROFILE

Sreeja Nair M. P., is currently a faculty in Computer Science and Engineering in Cochin university College of Engineering Kuttanad, Cochin University of Science and Technology after her BTech and MTech. She is also a research scholar in the same university. Her research work is in the area network security application Layer DDoS Attack.Her area of interests are network security, Machine learning

Dr. Mathew Cherian is currently a Faculty in Cochin university College of Engineering Kuttanad, Cochin University of Science and Technology. He completed his Phd from IIT Madras. He is guiding many research scholars in the college. His interested areas are Supply Chain Management, Decision-Making and OR.

Dr.Preetha Mathew K., is currently a Faculty in Cochin university College of Engineering Kuttanad, Cochin University of Science and Technology .She completed her Phd from IIT Madras. She is guiding many research scholars in the college. Her interested Areas are cryptography, Block chain and Machine learning.