PREVENTING DISTRIBUTED DENIAL OF SERVICE ATTACKS IN CLOUD ENVIRONMENTS

Subramaniam.T.K[1*], Deepa.B[2]

[*1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

ABSTRACT

Distributed-Denial of Service (DDoS) is a key intimidation to network security. Network is a group of nodes that interrelate with each other for switch over the information. This information is necessary for that node is reserved confidentially. Attacker in the system may capture this private information and distorted. So security is the major issue. There are several security attacks in network. One of the major intimidations to internet examine is DDoS attack. It is a malevolent effort to suspending or suspends services to destination node. DDoS or DoS is an effort to create network resource or the machine is busy to its intentional user. Numerous thoughts are developed for avoid the DDoS or DoS. DDoS occur in two different behaviors they may happen obviously or it may due to some attackers .Various schemes are developed defense against to this attack. The Main focus of paper is present basis of DDoS attack, DDoS attack types, and DDoS attack components, intrusion prevention system for DDoS.

KEYWORDS

DoS, confidentiality, DDoS, Security, botnets

1. INTRODUCTION

In the network computer system's large number of computer system is associated with different machine that are geographically distributed network. Network attacks, threats security are major difficulty in computer system networks. The network security or web services are method of earning unofficial admittance to network. And also the attacks take part in a chief role in security. The attacks are categorized into two associated type's that is passive attacks and active attacks. The network impostor capture data travelling through the network is said to be a passive attack. Idle scan, wire patter, and port scanner are some of examples of passive attacks. Intruder instructs command to disrupt networks usual operation. This is called active attacks. Man-in-middle attack, Denial-of-service attack, spoofing are some of the examples of active attacks. This attack can be accepted in various ways and various policies. The essential facet would be to block victim's network system and thus make it unreachable by other client computer system [1]. There are numerous ways of creating service that are unavailable to target users. Rather than just flooding with copious IP packets. The dupe could also be hit at various loopholes [12]. By creating it unstable which may depends on the nature of the attack. There are several manifestations of Distributed Denial of Service attacks but they eventually have the same purpose that is to deny or corrupt users' ability to legitimately access network DoS

DOI:10.5121/ijitca.2016.6203

2. Related Work

2.1. DDoS Attack Overview

The Denial of service attack is one of the types of active attack. The Denial of service attacks which revenue that the attackers can send certain messages which is vulnerable to the system. Sometimes they send packets to the target system which may result in failure [1]. As the remediation of susceptibility and reduction of performance to commerce systems, the harm of common DoS attacks becomes relatively minor. A Distributed Denial of Service attacks is implemented on the source of DoS attack and numerous dispersed attack sources. Usually, the attackers use a huge number of controlled bots dispersed in different locations to start on a great number of denial of service attacks to a lone target or several targets. With the quick growth of botnets in modern years, the attack traffic scale caused by Distributed Denial of Service attacks has been rising, with the target system, including not only industry servers, but also Internet infrastructures such as routers, firewalls and Domain Name Server systems as well as network bandwidth. The attack pressure sphere has also become broader.

2.2. Attack methods

In computer network they use a protocol for called transmission control protocol .The packets are transferred through TCP. The attacker can send one or more attack packets to the network. This will cause the target servers and network resources and also overloads the server. These are the vital principles of Distributed Denial of Service attacks. The key reason is inflexible avoidance of DDoS attacks deception in the combination up of justifiable traffic and illegitimate traffic. It is difficult to discover the attack packets from the diverse traffic in the avoidance progression, particularly when the harass message packets masquerade to be normal messages. For exemplar, in signature -based pattern corresponding Intrusion Detection system, it is not easy to differentiate illegitimate packets from legitimate messages packets. In universal, according to the uniqueness, DDoS attacks can be divided into the following types:

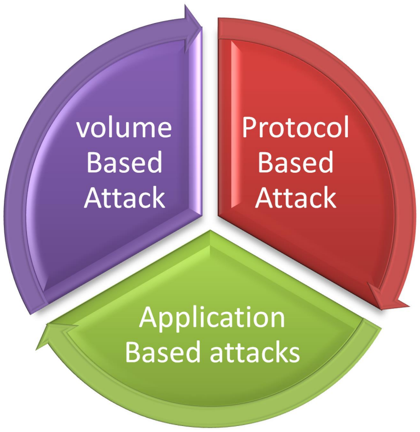


Fig 1: Attack Methods

2.2.1. Volume-based attacks Distributed Denial of Service attacks

This type sends huge collection of junk data packets to cause the network devices to be overloaded, which leads to enlarge the networks bandwidth. Hence further more incoming requests are dropped and network will be blocked.

2.2.2 Protocol-based attacks

The most familiar forms of denial of service attack are traffic flooding attacks. N traffic flooding attack the attackers send a great number of ostensibly legitimate UDP, Transmission Control Protocol/Internet Protocol, ICPM packets in network host. This will cause a more traffic in the networksystem.

2.2.3. Application-based attacks

The attacks of this type often mail the consequent application-layer; main focus of this system attack is to deny the service of application layer. The low rate of traffic can also lead serious degradation of service.

3. Cloud environment and deployment model

Cloud computing is a technology that build a most important changes in business and IT industry. Even though running application and programs on individual system we can run it on cloud environment. Cloud computing is helps business people to deploy their services with low cost. Cloud computing is beneficial to business and IT industry by low cost investments. It act as a pay as service model whenever they needs service they access it from the cloud [5]. They need to pay according to their usage

Cloud computing are deployed as three types of services such that platform as a service, infrastructure as a service and application/software as a service.

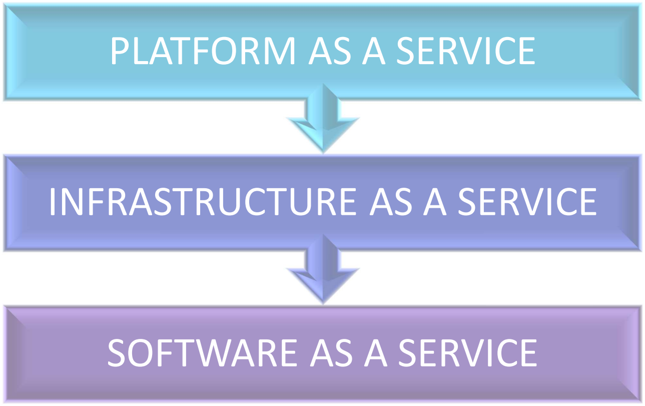


Fig 2: cloud Deployment Model

3.1 Platform as a Service (PaaS):

This Platform as a Service provides an environment for developing a service. This environment consists of predefined set of operating system and application software's. The user of cloud can easily develop applications in this platform. It also provides platforms like mysql, Linux, etc.

3.2 Infrastructure as a service (IaaS):

This communications service offers set of infrastructure such as storage space and computing devices for network. This infrastructure service also provides a data centers and also provides a virtual storage space and data centers.

3.3 Application / software as a service (SaaS):

This environment provides an application or software to the end users. The user of cloud can access the service by on demand requests to cloud servers. They no need to acquire narrative software's and authorization for that application software. They access the application for rent. The single instance of application in cloud environments can able to run in a multiple client system.

4. DDOS ATTACKS IN CLOUD ENVIRONMENTS

The denial of service attacks happens in cloud computing infrastructure. This might occur obviously or for a while it may occur due to botnets or professional attacker. This attack may be prepared for several reasons. This may happen when the service request to cloud environments [6].

4.1 Types of DDoS attacks:

Distributed denial of attack has several types such as UDP flood, ICMP flood, SYN flood, Ping of Death, slowloris, HTTP flood attacks.

4.1.1 UDP Flood Attack:

This type of denial of service attack happens in User Data Gram protocol .It establish a session less connection by user datagram protocol. It enters into any one of the port in host computer with one or more numerous UDP packets. This session-less service roots the port that will require to confirm the port wether the packets will be reached or nor [5] [6].

4.1.2 ICMP Flood Attacks:

Internet Control Message Protocol Attacks. Normally ping request packets are send to destination host to check whether the host is connected are not. This is identified by ping replies. Attackers send more number of packets without waiting for replies. This consumes more bandwidth and cause ICMP flood attacks.

4.1.3 SYN Flood Attacks:

In general TCP which follows a three way handshaking. The client send synchronization request to destination host server. The servers respond to the clients by sending synchronization acknowledgements. Then the client will launch the Synchronization Acknowledgement. This attacks will occur by the client will send one or more SYN request to single or extra numbers of host destination server and does not respond to the Acknowledgment request. The host servers system that continuously was waiting for a reply. This will cause a Synchronization Flood DDoS attacks.

4.1.4 Ping of Death Attacks:

The attacker approved away this attack by throw a malware attacking ping request packets to one or more computer. There is limit for packet length. This will cause the buffer over in the host. This will results in DDoS attacks.

4.1.5 Slowloris Attacks:

Slowloris creates a constant connection to the host server. This will only send half of request to target server. The target host server is open for ever wrong connection. It invariably more number of HTTP request but never complete the request.

4.1.6 HTTP flood Attacks:

The attacker carried out these attacks by GET and POST methods. It tries to complete a resource request with greatest number of resources. These will fallout in HTTP Flood DDoS attacks.

5. LITERATURE REVIEW

5.1 Existing Prevention Techniques

Intrusion Prevention System: Intrusion prevention Technique which can be efficiently used to detect the DDoS attack. An intrusion prevention technique which follows a combination of one or more number of detection mechanisms it includes signature based detection, firewall based prevention, and Anomaly based detection [7] [11].

5.1.1 Signature Based Attack:

In computer network, the traffic of the network is monitored along with signature pattern. The attacks pattern is compared with help of signature database. The database encloses one or more number pre-defined signatures. If the traffics match with database signature traffic it will take necessary steps to block the attacks.

5.1.2 Firewalls:

Firewalls are one of the methods of Intrusion Prevention System. The main idea of using firewall within the environment to impose endeavour strategy and preserve association state information for genuine users both internally and also externally and not to prevent high volume DoS / DDoS style attacks [7][12].

FIREWALLS
EXISTING TECHNIQUES
FUZZY BASED ECHNIQUE
SIGNATURE BASED ATTACK
ANAMOLY BASED PREVENTION

Fig 3: Existing Techniques

5.1.3 Anomaly based Detection:

Anomaly based detection is supposed to be a profile based signature monitors system. It observes the network traffic continuously .If the traffic mismatches the existing normal traffic. It consider as an attack. And its blocks the concurrent networks to prevent a DDoS attack.

5.1.4 Fuzzy based technique:

Fuzzy is a software tool to test the end user application and protocols. Each time there is a situation to implement a new protocol or software or any application. It must be tested with fuzzy tools. The tool will decide whether it can be implemented in real-time and it wether it is a secure one or not [17].

Filter based approach: Flow level filter is used to detect the low rate DDoS attack. Low rate DDoS attack which gradually increase the traffic rate and attack the network host. Flow level filter which blocks the DDoS attacks [8] [13].

6. PROPOSED PREVENTION TECHNIQUES

6.1 Software Puzzle:

A software puzzle is a novel technology. The end users or clients of a cloud need to solve a puzzle before granting a service. Normally cloud computing offers on demand services to end users, whenever user needs a service or any other thing they request to cloud server. The cloud service provider or cloud server offers a service when the cloud users request a service. The attacks may occur easily in cloud environment [19]. These DDoS attacks that is critical to cloud servers. The proposed system software puzzle that may help to prevent those DDoS attacks.

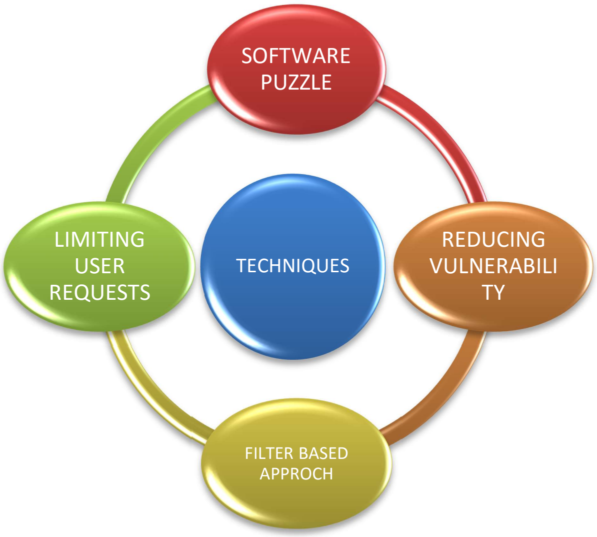


Fig 4: Proposed Technique

In this software puzzle scheme the end user request to the server that is cloud server or cloud service providers. The service provider or server responses to the particular client with software puzzle. The client needs to solve the puzzle where it is send by the server. The client again sends it to the server [19]. The server verifies whether the puzzle is correct or incorrect. If it is correct the server offers the requested service to the end user.

By using this software puzzle we can prevent the DDoS attacks. The DDoS attacks sometimes generated from computer machines is completed blocked because of software puzzle. The machines cannot able to solve the software puzzle. Hence generating DDoS from the machines is completed blocked.

6.2 Reducing vulnerability by network mechanism:

This also helps in reducing vulnerability of DDoS attack happening in the network. In computer network and web services there is a more number of loop holes that are supplementary susceptible to the system security. This provides a ways for happening of attacks. The usage of queue in computer network is completely avoided. These are more vulnerable to the environments.

In computer network they use a finite queue whenever the incoming inputs or incoming request increase the queue gets filled. Hence they cannot process the further more requests. This unprocessed request also creates vulnerability of happening DDoS attacks. If the system uses a queues it must have fixing their job sizes otherwise eliminate their queuing model [20].The First Come First Serve queuing system is vulnerable o DDS attack. If size of job is too big it process only the first inwards job. Hence further more requests are not processed by system .It results in DDoS attacks.

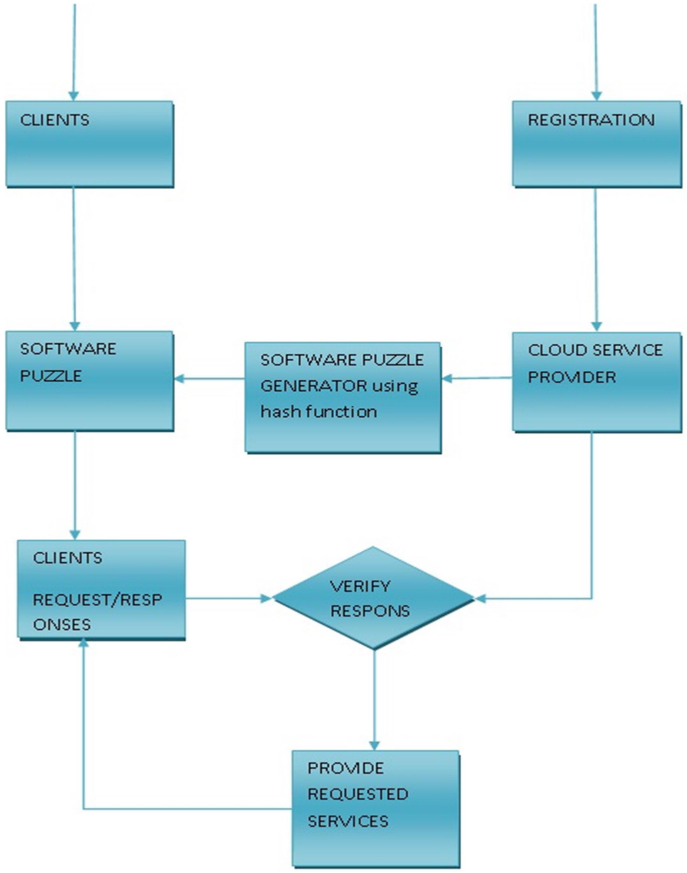

CLIENTS
REGISTRATION
SOFTWARE PUZZLE
SOFTWARE PUZZLE GENERATOR using hash function
CLOUD SERVICE PROVIDER
CLIENTS REQUEST/RESP ONSES
VERIFY RESPONS
PROVIDE REQUESTED SERVICES

Fig 5: flow diagram

Software puzzle scheme is used to prevent the DDoS attacks. Here no queuing system is to be used and also no job or process is to be waited. When ever needed they request it solve it and get a service .in this system there no vulnerability.

The flow diagram describes about that the client would register with the service provider. The client can give request to service provider. The service provider generates a puzzle by using a hash function. The client must solve the puzzle before they access services in cloud

6.3 Threshold based prevention:

The Denial of service (DoS) attack can be performed in a simple way by sending a large number of requests to the server. Sometimes it may be completed through with help of softwares by attackers. On occasion machine made attacks can also be happened. This can also be prohibited by threshold based avoidance method. The end users of system can given only a particular amount of request in particular time period [10]. If it reaches the particular threshold value the user will be blocked.

7. CONCLUSION

Denial of service and Distributed Denial f service has been completed prevented before it going to occurs. These types of attacks are hard to detect and recover after the attacks have been occurred. This is impossible to detect and also recover from attacks. The proposed work which follows three types of prevention mechanism which completely prevent the denial of service attack before the attack event occurs.

REFERENCES

[1] Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks", IEEE Communications Letters, Vol. 17, No. 1, January 2013.

[2] zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE,andRenPingLiu,Member, IEEE," A System for Denial-of-Service Attack Detection Based on MultivariateCorrelation Analysis.", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[3] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM," Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks", IEEE/ACM Transactions On Networking, Vol. 20, No. 3, June 2012.

[4] Moti Geva, Amir Herzberg, and Yehoshua Gev |," Bandwidth Distributed Denial of Service: Attacks and Defenses", Copublished by the IEEE Computer and Reliability Societies January/February 2014 .

[5] Zahid Anwar and Asad Waqar Malik," Can a DDoS Attack Meltdown My Data Center?A Simulation Study and Defense Strategies", Ieee Communications Letters, Vol. 18, No. 7, July 2014.

[6] Shui Yu, Senior Member, IEEE, Yonghong Tian, Senior Member, IEEE,Song Guo, Senior Member, IEEE, and Dapeng Oliver Wu, Fellow, IEEE," Can We Beat DDoS Attacks in Clouds?", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 9, September 2014.

[7] Xinlei Ma and Yonghong Chen," DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy", IEEE Communications Letters, Vol. 18, No. 1, January 2014.

[8] Markku Antikainen, Tuomas Aura, and Mikko Särelä," Denial-of-Service Attacks in Bloom-Filter-BasedForwarding", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[9] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker," Detecting Spam Zombies byMonitoring Outgoing Messages", IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[10] Shui Yu, Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Weijia Jia, Senior Member, IEEE, Song Guo, Senior Member, IEEE, Yong Xiang, and Feilong Tang," Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient ", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.

[11] G.V. Nadiammai, M. Hemalatha," Effective approach toward Intrusion Detection System using data mining techniques", Egyptian Informatics Journal (2014) 15, 37–50.

[12] Jérôme François, Issam Aib, Member, IEEE, and Raouf Boutaba, Fellow, IEEE, " FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks" IEEE/ACM Transactions On Networking, Vol. 20, No. 6, December 2012 .

[13] Changwang Zhang, Zhiping Cai, Weifeng Chen , Xiapu Luo, Jianping Yin," Flow level detection and filtering of low-rate DDoS", Computer Networks 56 (2012) 3417–3431

[14] Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas,"Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 3, May/June 2012

[15] Jingtang Luo, Xiaolong Yang, Senior Member, IEEE, Jin Wang, Member, IEEE,JieXu,Member, IEEE, Jian Sun, Member, IEEE, and Keping Long, Senior Member, IEEE," On a Mathematical

Model for Low-Rate Shrew DDoS", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7, July 2014.

[16] Hongbin Luo, Yi Lin, and Hongke Zhang, Beijing Jiaotong University Moshe Zukerman, City University of Hong Kong," Preventing DDoS Attacks by Identifier/Locator Separation", IEEE Network • November/December 2013.

[17] Tero Rontti, Anna-Maija Juuso, and Ari Takanen, Codenomicon Ltd. ," Preventing DoS Attacks in NGN Networks with Proactive Specification-Based Fuzzing ", IEEE Communications Magazine • September 2012.

[18] Jin Tang, Member, IEEE, Yu Cheng, Senior Member, IEEE, Yong Hao, and Wei Song, Member, IEEE. ," SIP Flooding Attack Detection witha Multi-Dimensional Sketch Design", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 6, November/December 2014

[19] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng ," Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015.

[20] Udi Ben-Porat, Student Member, IEEE, Anat Bremler-Barr, Member, IEEE, and Hanoch Levy, Member, IEEE. ," Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks", IEEE Transactions On Computers, Vol. 62, No. 5, May 2013.

[21] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds"2013.

[22] Apurva Shitoot, Sanjay Sahu, Rahul Chawda, "Security Aspects in Cloud Computing", IJETT, Volume 6 number 3 - Dec 2013.

[23] Morsy MA, Grundy J, Müller I ," An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia",2010.

[24] Jansen WA ," Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa", Kauai, HI. IEEE Computer Society, Washington, DC,USA, pp 1–10,2011.

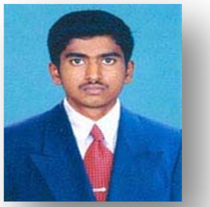
[25] B. Barak et al., "On the (Im)possibility of obfuscating programs," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2139. Berlin, Germany: Springer-Verlag, 2001, pp. 1–18.

[26] H.-Y. Tsai, Y.-L. Huang, and D. Wagner, "A graph approach to quantitative analysis of control-flow obfuscating transformations," IEEE Trans. Inf. Forensics Security, vol. 4, no. 2, pp. 257–267, Jun. 2009.

[27] Subramaniam.T.K, Deepa.B, "A Survey On DDOS Attack Detection And Prevention Methodology" International Journal of Intellectual Advancements and Research in Engineering Computations, JUNE 2015.

[28] Subramaniam.T.K, Deepa.B, "A Review towards DDoS Prevention and Detection Methodology" International Journal of Computational Science and Information Technology (IJCSITY) Vol.3,No.1/2/3,August 2015.

AUTHORS:



T.K.SUBRAMANIAM received the B.Tech degree in Information technology from Nandha Engineering College in the year 2014.He is currently doing his M.E Computer science and Engineering in Nandha engineering college, Erode, India. His area of interest is web services. He has published many journal papers.

B.DEEPA received the M.E degree in Computer Science and Engineering from Nandha Engineering College in the year 2011.She is currently working as Assistant Professor in Nandha Engineering College, Erode, India. She has published many international and national research papers. Her area is Network security and web services. She has depth knowledge of her research area.