Journal of Advances in Science and Technology
Vol. 17, Issue No. 1, March-2020, ISSN 2230-9659

A Review on Artificial Intelligence Based Active Defense System against Online Service Attacks

Bhargava R.[1]* Dr. Yash Pal Singh[2]

[1] PhD Student, Kalinga University, Raipur

[2] PhD Guide, Kalinga University, Raipur

Abstract – Artificial intelligence technologies have been increasingly popular in recent years, with applications in computer vision, natural language processing, automated driving, and other disciplines. Artificial intelligence systems, on the other hand, are subject to adversarial assaults, which restricts the use of AI technology in critical security areas. As a result, strengthening the resilience of AI systems against adversarial assaults has become increasingly essential in AI development.The goal of this paper is to provide a thorough overview of recent research on adversarial attack and defensive methods in deep learning. This article explains adversarial attack strategies in the training and testing stages of the target model, according to the distinct stages where the adversarial assault happened. The applications of adversarial attack technologies are then sorted out. Computer vision, natural language processing, cyberspace security, and the physical environment are all areas where researchers are working. Finally, we divide the known adversarial defensive strategies into three categories: data modification, model modification, and the use of auxiliary tools.

Keywords – Artificial Intelligence; Deep Learning; Defense Method; DDOSAttacks; DDOS Defense; DDOS Prevention

---------------------------------x---------------------------------

1. INTRODUCTION

Services offered online, that varies from easy mail systems to complicated smart grids, carries most of traffic on internet, take up an important part in our daily social lifeline. Meanwhile, in years to come amount of networked gadgets and number of network traffic are predicted to rise exponentially. Even though such practices greatly facilitates human existence, but can invites easy access for malicious attacks and malwares [1]. Adversaries could get equipped with destructive power with the help of only a small portion of compromised network. As per CISCO's white paper [2], amount of distributed denial of service (DDoS) breach will increase to 15.4 million in 2023 all across globe, making online service security and privacy one of critical research area. Age old practices that involves static defenses like widely applied firewall can address threats in a fixed way. Usually communication systems grows to be heterogeneous and very large in sized, such passive defense approach is apparently insufficient in keeping up with development of always evolving new types of attacks. Always rising common vulnerabilities and exposures (CVE) as per national vulnerability database (NVD) precisely assist this view and put up request to defenders for new developments in this field. Hence, active defense is suggested as a decision makers in reshaping defencd-attack confrontation and eradicate attackers' uneven benefits. Instead of developing a fixed defense mechanism to repulse attacks, active defense constitutes great significance to actively evolving protected and secured system. Such dynamic features drives system to unpredictability and hence could overturn a large number of cyber assault. Undoubtedly, it needs good amount of efforts of defenders to determine realize and apply dynamic defense schemes in very complicated network atmosphere, which hinders development and evolvement of active defense for a long period of time. Meanwhile, for activating defense for large-scale implementation of artificial intelligence (AI) infuses new vitality. Post receiving help from AI, particularly learning technologies such as deep learning [4], and reinforcement learning (RL) [3], defense mechanism can be built autonomously by learning from historical data available with data bases or data banks.

But, recent local attack defenses (LADs) still not possesses negligible deficiencies. Most trending problem that lurks is the one to be resolved is low self-security and privacy of defenders as researchers and scientists usually focusses on securing protected system, whereas security of defense technique is overlooked. Currently trending and emerging advanced persistent threat (APT) arrangement, deductive attack can predict and undermine defense policies. Once defense machinery crashes, entire system gets compromised thereby jeopardizes goals of communications. Few LADs [5] have implemented diverse compilers or operating systems to soften this fatal risk. However diversity needs financially effected efforts in preparing sufficient disparate system variances. Even though after defenders acquires sufficient resources, security behavioral pattern of these variants is still remains under suspicious as well as knowledge gathering of attackers, and large-scale adjustment or deployment becomes very complicated to attain. Such difficulties highly hampers further security enhancement and have been keeping researchers wondering for an elongated period of time. This leads to our aim: for designing a novel defense approaches that is capable in guarding itself against deductive attacks. The ability in protecting defense mechanism autonomously as endogenous security, and as per capability of system to protect and secure online system as exogenous security. With this perspective, we suggest a new endogenous security defense strategies called learning-enhanced spatio-temporal strategy mutation (LSSM) that can adaptively attain randomness of defense strategy in a huge heterogeneous network atmosphere.

2. REVIEWOF WORKS

2.1. DDOS Attacks and Defenses

Breaches or attack of DDoS types effects entire layers of cloud infrastructure (SaaS, IaaS and PaaS) and can happen remotely or inside [6] - [8]. An outer cloud-dependent DDoS breaches initiates from outer side of cloud situations and aims at services that are cloud-based. Such types of cyber assault effects services accessibility. Most influenced layers in cloud infrastructure from an outer DDoS breaches were PaaS and SaaS layers. Cyber assault from inside of cloud-dependent DDoS occurs within framework of cloud systems, principally in IaaS and PaaS and substrates, and could takes place in many various methods. As an example, Adversaries can exploit times intervals for cloud services testing of particular sellers or clients. Hence, validated client from within conditions of cloud can releases a DoS attack on inside of casualty's machine. Once more, sharing effected simulated appliances pictures can allow an adversaries in controlling and using contaminated virtual machines in executing an inside DDoS breaches that is focused on machine within a similar cloud processing infrastructure. Different types of attacks is included in DDoS. Portrayals of such cyber attacking and suggested handy barrier instruments in cloud framework were introduced under accompanying segments.

a. Attack of IP spoofing types

With regards to spoofing attack on Internet Protocol (IP) [9], sending of bundles amongst cloud server and end-client could be blocked and their headers altered with end goal such that source field in IP in chunk of IP is generated by either an authentic address of IP, with unavailable IP address. Hence, server responds to real client machine, that effects it, or server will be unable in completing exchange to inaccessible IP address, thus effecting assets of server systems. Ensuing these cyber assault is complicated due to pretentious address of source field in bundle of IP. Schemes in identifying attack of IP spoofing kind can be implemented in system assets or layer of PaaS on layer of IaaS.

Due to troubling of altering as well as updating various kinds of assets in systems in cloud infrastructure, jump check separating (HCF) [10] can be used to identify spoofed IPs from genuine IPs in layers of PaaS. HCF regulates amount of jumps depending on calculation of Time to Live (TTL) portion present in header of Internet Protocol. IP-to-bounce check (IP2HC) configuring is executed to recognize bundle of spoofed data. Research and study done by Wang et al. [10] depicted 90% of location that were spoofed can be recognized by deploying HCF methods. A single disadvantage in such technique is, attackers could assemble their own IP2HC configuration to avoid being confronted by HCF. Trust based method in handling identify spoofed IP locations could use within entrance switches on layers of IaaS [11], yet additionally good arrangement ought to be proposed to recognize IP spoofing in appropriation switches.

b. Attack of SYN flooding types

An Interconnection that initiates with handshake in three different way is Transmission Control Protocol (TCP). Distinctive three-way handshake amongst server and an authentic user initiates by transmitting a connection appeal by authenticated and valid user to server in terms of synchronization (SYN) message signals. Later, server identifies SYN by responding with (SYN-ACK) requesting to these users. Lastly, such user transmit an ACK appeal to server for establishing concerned connections. If an attacker drives a large amount of data packets to server however keeps procedure of three way handshaking incomplete, SYN flooding takes place. Consequently, server keeps waiting to executes process for entire packets of information, making server incapable compute valid requests. Moreover, by transmitting packets along with a spoofed IP address SYN flooding can be carried out. Sniffing attack is included as a type of SYN flooding attack. In this kind of attack, Adversaries sends a data packet including forecasted sequence number of an active connection of TCP having IP address that is spoofed. Hence, server cannot respond to that request, influencing behavior of resource in cloud based systems.

In IaaS and PaaS layers various guard systems for safeguarding against SYN flooding attack can be implemented [12]. SYN store concept [13], can be taken into consideration within PaaS layer, that configures bonding with a real solicitation, still such situations creates rise in inactivity by upto 15%. To identify a SYN flooding attack SYN treats resistance instrument [13] is one more concept put forth for safeguarding element in PaaS layer, however it decreases exhibition of cloud infrastructure. Decreasing an hour of SYN got to lower the break is proposed measure of PaaS guard, but in due process genuine ACK data parcels can be lost. Additionally, few of instruments used for identification, including dynamic observing, firewall and sifting, can be applied in layers of IaaS.

Sifting is a successful technique to forestall a SYN flooding attack by designing inside and outer switch interfaces, however this strategy isn't dependable because of its restricted use. Instruments of firewall in layers of IaaS relies upon parting TCP association, yet such types of connections could influence exhibition of systems administration framework. A functioning checking instrument [14] could be used in IaaS layer to screen traffic of TCP/IP and respond in instances of SYN flooding. In any case, this methodology relies upon the SYN treats component, which prompts diminished execution of cloud assets.

c. Attack of Smurf type

In this, Adversaries transmits an huge amount of Internet Control Message Protocol (ICMP) reverberation demands. Such solicitations were deceived with end goal as if its source IP address is IP of casualty, and IP goal address is communicated IP address. Accordingly, casualty would overflow with communicate addresses. Most pessimistic scenario happens if quantity of hosts that answer to ICMP reverberation demands was excessively enormous. Forestalling such types of assault is troublesome, yet it tends to be moderated by two unique systems. The first suggested protection instrument in layers of IaaS arranges switches to impair IP-coordinated communicate rules; thus such kind impaires of course in current switches. Be that as it may, attacker can use undermined gadgets in cloud infrastructure as a middle person to transmit reverberation solicitations of ICMP to communicate IP address locally, in this manner completing an inward cloud-based DoS attack. Arranging the switch in the IaaS layer can't forestall a smurf attack. Thusly, a second protection component is required, which is arranging the working frameworks in the PaaS layer so that there is no reaction to the ICMP bundles sent to the IP communicate addresses.

d. Buffer flood attack

In a cushion flood attack, the attacker sends an executable code to the casualty so as to exploit support flood weakness. Therefore, casualty's machine can become constrained by an attacker. Adversaries can either utilize contaminated machine or hurt casualty's machine to play out inner cloud-dependent attack of DDoS type. For resistance components to forestall cushion flood powerlessness can be utilized in the SaaS layer [15]. The principal instrument is forestalling such weakness when composing the source code [15]; in any case, time utilization is a confinement. Executing regulations of cluster limits is an another suggested barrier instrument; such concept comprises of inspecting compiler and memory access thereby utilizing wellbeing language. Third safeguard system is runtime arrangements, that could either change arrival address to identify powerlessness or gauge cushion limits at that point play out a check of limits of runtime. Fourth suggested safeguard instrument in SaaS layer is investigating dynamic and static code to identify user’s defenselessness in such substrates.

e. Attack of Ping of death type

With such type, attacker transmit an IP packets comprising size larger to that of restriction constituted in IP convention, that is more than 65,535 bytes. Taking care of a curiously large parcel influences the casualty's machine inside the cloud framework just as the assets of the cloud framework. Ongoing system assets and working frameworks ignore any IP parcels bigger than 65,535 bytes. In this way, such attacks are not as of now influencing any cloud framework layers.

f. Attack of Land type

Such cyber assault uses programs in "Land.c" in transmitting manufactured TCP SYN bundles with casualty's IP address in goal and source. For this situation, machine would crashes framework after getting a solicitation from itself. These kinds of attack was forestalled into ongoing systems administration gadgets and working frameworks by excluding ICMP bundles containing similar IP address in goal and source fields. Therefore, here isn’t any requirement about land attack resistance instrument to be used in entire cloud framework’s layer. In any case, way toward dropping after checking large number of ICMP solicitations can effect assets of casualty's machine in PaaS layer or systems administration assets in IaaS layer.

g. Attack of Teardrop type

In this kind, it uses "Teardrop.c" program transmitting un authenticated estimation of covering in IP parts within header of TCP’s packets. Accordingly, machine of casualty in cloud system surely crashes in re-get together procedure. Ongoing working frameworks and system assets can deal with such attacks. Thusly, tear attacks does not effects any cloud processing’s layer.

2.2. DDOS Prevention Approaches

As per [9], machine learning [15] can be utilized to forestall DDOS attacks in a robotized design. Our proposed framework has the accompanying highlights:

- Fully mechanized framework to forestall DDOS attacks.
- Focus on asset use as opposed to bundle observing.
- For attack recognition applying Artificial Neural Network as well as putting away their outcome in example large database for later reference. Suggested framework comprises of accompanying advances:
- An overhead observing hub that persistently screens framework assets (CPU, NETWORK). On off chance that used asset is more than given edge esteem, approaching bundles are recognized as strange.
- A traffic checking hub that constantly screens the bundles from various layers of system .Bundles received by various layers were broke down, hence we get an adequate measure of information for dissecting whether solicitation was authentic else ill-conceived.
- These server which is focal part of framework, executes two fundamental undertakings: they gets information by traffic and burden checking framework thereby storing it for additional preparing. Besides, they persistently screens framework. In such event that framework is seen as working in ordinary condition, at that point standard profile for these solicitations is kept up and on the off chance that framework is identified to be attacked, at that point element extricated from traffic and heap observing framework is kept inside Database which is not complex.
- Benchmark profile information is stored in Database and data removed through traffic and burden observing frameworks which is utilized considering contribution in preparing calculations.
- Standard profile information now applies ANN in preparing calculation as well as recognize contrast amongst typical parcel and malevolent bundle that could utilizes in forestalling attack.
- The sifting hub utilizes the calculation delivered through ANN for channeling and dropping noxious parcels.
- Observing hub was fundamentally an internet application that encourages administration in ceaselessly dealing with condition of framework.

DDOS attack identification is a perplexing and entangled issue for cloud computing innovation. Regardless of utilizing different procedures, attacks of DDOS is amongst major defenseless attacks. Machine learning based artificial neural system could utilizes in accomplishing a phenomenal arrangement as it utilizes a computerized framework. As opposed to breaking down system traffic, the fundamental point of this method is to screen assets which makes it an effective procedure.

2.3. Attack-Defense Profile for online services

As it is evident from upper middle potion of detailed description ofillustration, online service system majorly constitutes one central server to deliver many services and various proxy servers to manage access to user. It must be notable that system could be largely multiple sized and complex in actual real time scenarios. As an instance, main server must very big cloud platform or data center in case of huge proportions video sharing services such as YouTube. But for briefness, we mainly aim at focusing on key constituent which are related with system security. With same regards, we could consider attacking process and development of attackers as many steps in sequence. In primary step adversaries gain access to target system through a through a manipulated user's details that we mentioned as spy. This spy stealthily collects proxy data such as port number or an in step second, and gives important victims for attacker in step three. Step fourth involves, attacker tracks their self-interest and institutes regulations create parallel attack patterns, executing particular attack resource scheduling and preparation. Lastly, in fifth step, botnet takeoffs attack as per pattern's instructions.

2.3.1. Technical Classification

Currently having learning-enhanced active defenses majorly delivers countermeasures for three categories of attack procedures as we named detection, prediction, and shuffle, respectively. Step 5 deals with Detection of unwanted or unauthorized access to various entities; step 4 involves prediction; and from step 1-3 includes shuffle prevents counter measuring spy applications, malware, etc. Detection: Such groups can be viewed as blending of network traffic filtration and AI, such as deep packet inspection (DPI) or (IDS) intrusion detection system. For regulating traffic Detection modules are implimented on borders of network. As large-scale botnets are always responsible for resourceexhausted cyber-attacks, learning-assisted methods like artificial neural networks (ANNs) [16], RL [3] and support vector machine (SVM) [1] can effectively assist defenders to optimize and create detection rules independently. As a result, traffic purification is attained with a botnet's malicious information being restricted, this known to be blocking capability. It is evident that detection schemes have a efficient and concise and structure, enabling defenders to effectively restrict botnet traffic in groups. However detection also infuses disadvantages like loss of instantaneous misjudgment rate and high-performance in parallel. Prediction: This category eventually executes from uses of game theory security and privacy. Depending on previously stored historical logs, defender succeeds in speculating attack pattern with the help of AI technique's support. Later both protected system and security policy can be set as per situation that arises. Due to this, loss is reduced, and expenses of hurling an attack outweigh their gains. Thus we refer such kind of defense effect as circumventive capability. Various prototypes, including green security game [18], hidden Markov model [17], subjective utility quantal response (SUQR) and Stackelberg security game (SSG) were suggested to show confrontation in real-world cyber arena. With regards to AI-assisted section, Sinha et al. [19] provided proof about feasibility of learning, and application of RL to prediction of both defenders and attackers are provided by Trejo et al. [20]. These illustrated research have given a way for future applicatory and theoretical and research. Briefly, by predicting malicious attacks prediction schemes effectively enhances security of systems, only bringing performance burden and relatively minute alteration of systems. But, tireless work done to identify a particular pattern of attack pattern can also drives defense system insensitive and inextensible in dynamically varying conditions. Shuffle: moving target defense (MTD) [21] based on Shuffle technologies were primarily referred to endure never ending stream of novel variants of cyber-attack. Contrary to other two groups, shuffle pays focusses more in making protected system diversified, stochastic, and dynamic, rather than analyzing adversaries [22], [23] as in case of remaining two. By filtering malicious traffic from botnets attacks are thwarted by Detection; prediction invalidates attacks by avoiding pattern of attack; by eliminating malicious spies attacks are neutralized with shuffle. Although prediction and detection consist of better performance of security, without counter attacking they repel cyber threats. Hypothetically, adversaries can continue initiating attacks always against prediction ad detection, while to shut attack down shuffle can within no time damages attack resources.

Referring such characteristics capability of counterattack, meaning that defenders can not only capable in protecting system but also inflicts harmful damage to attackers. As it is clear that, shuffle techniques embalmed learning-enhanced do not solely based on information of malicious adversaries to increase safety of systems, thereby adapting better to varying attack patterns and fulfill online services requirements.

3. DEFENSESTRATEGY

Researchers have proposed a number of adversarial attack defense strategies, which can bedivided into the three main categories, i.e., modifying data, modifying models and using auxiliarytools. We describe them in details, respectively.

3.1. Modifying Data

These strategies refer to modifying the training dataset in the training stage or changing the inputdata in the testing stage. It includes the following:

- Adversarial Training
- Gradient Hiding
- Data Compression
- Data Randomization

All these methods helps to reduce breaching by simply training the artificial intelligence and forming new database for example, in data randomization strategy "Xie et al. [45] demonstrated that the operation of random resizing adversarial samples can reduce The effectiveness of adversarial samples. Similarly, adding some random textures to the adversarial Samples can also reduce their deception to the network model. Wang et al. [46] used a data conversion Module separated from the network model to eliminate the possible adversarial disturbance in the Image, and conducted data expansion operations in the training process, such as adding some Gaussian Randomization processing, which could slightly improve the robustness of the network model".

3.2. Modifying Model

We can modify the neural network model, such as regularization, defensive distillation, feature Squeezing, deep contractive network and mask defense. For example, in mask defense "Gao et al. [53] proposed to insert a mask layer before processing the classified network model. This mask layer trained the original images and corresponding adversarial samples and encoded the Differences between these images and the output features of the previous network model layer. It is Generally believed that the most important weight in the additional layer corresponds to the most Sensitive feature in the network. Therefore, in the final classification, these features are masked by Forcing the additional layers with a primary weight of zero. In this way, the deviation of classification Results caused by adversarial samples can be shielded".

3.3. Using Auxiliary Tool

This approach refers to using additional tools as an auxiliary tool to the neural network model,Including defense-GAN, Magnet and high-level representation guided denoiser.

4. CONCLUSION

Since Szegedy et al. proposed that machine learning algorithms are vulnerable to adversarialAttacks, researchers have conducted a large number of studies on adversarial attacks and defenseMethods and produced good results". In this paper, we reviewed DDOS attacks and defenses and DDOS preventionapproaches. Furthermore, we summarize the defensestrategy against these breaches that can be concluded in three ways - modifying data, modeling data and through auxiliary tools. Each od them helps in either reduce or prevent any foreign substance to connect with network securities but ensuring nothing is interfering with the security networks becomes a hard task. Therefore, the key to ensuring the security of AI technology in various applications is to Deeply research the adversarial attack technology and propose more efficient defense strategies.

REFERENCES

[1]. K. Singh et. al. (2018). "User Behavior Analytics-Based Classification of Application Layer HTTP-GET Flood Attacks," J. Network and Computer Applications, vol. 112, pp. 97–114.

[2]. K. K. Trejo et. al. (2018). "Adapting Attackers and Defenders Patrolling Strategies: A Reinforcement Learning Approach for Stackelberg Security Games," J. Computer and System Sciences, vol. 95, no. 99, 2018, pp. 35–54.

[3]. M. N. Kurt et. al. (2019). "Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5174–85.

[4]. S. Rezaei et. al. (2019). "Deep Learning for Encrypted Traffic Classi- fication: An Overview," IEEE Commun. Mag., vol. 57, no. 5, pp. 76–81.

[5]. J. Hong et. al. (2016) "Assessing the Effectiveness of Moving Target Defenses Using Security Models," IEEE Trans. Dependable and Secure Computing, vol. 13, no. 2, pp. 163–77.

[6]. Y. Ghebghoub, S. Oukid, and O. Boussaid (2013). "A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6.

[7]. Raj Kumar P. Arun, S. Selvakumar (2009). "Distributed Denial of service threat in collaborative environment- A survey on DDOS tools and Traceback mechanism", IEEE International Advance Computing Conference.

[8]. Mr. S. Karthik, Prof J.J. Shah (2014). "Analysis of Simulation of DDOS Attack in Cloud", Information Communication and Embedded Systems (ICICES), 2014 International Conference.

[9]. Stefan Seufert and Darragh O'Brien (2007). "Machine Learning for Automatic Defence against Distributed Denial of Service Attacks", ICC 2007 proceedings.

[10]. Chris Sinclair, Lyn Pierce, Sara Matzner (1999). "An Application of Machine Learning to Network Intrusion Detection". Phoenix, AZ 06 Dec 1999-10 Dec 1999

[11]. J. Burges (1998). "A tutorial on support vector machines for pattern recognition", Data Mining and Knowledge Discovery, vol. 2, pp. 12 1- 167.

[12]. Kamarularifin AbdJalil, Muhammad Hilmi Kamarudin, Mohamad Noorman Masrek (2010). "Comparison of Machine Learning Algorithms Performance in Detecting Network Intrusion", 2010 International Conference on Networking and Information Technology

[13]. Jayveer Singh, Manisha J. Nene (2013). "A Survey on Machine Learning Techniques for Intrusion Detection Systems", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[14]. Sujay Apale, Rupesh Kamble, Manoj Ghodekar, Hitesh Nemade, Rina Waghmode; "Defense Mechanism For Ddos Attack Through Machine Learning", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308

[15]. Sergio Armando Gutierrez, John Willian Branch Grupo GIDIA, "Application of Machine Learning Techniques to Distributed Denial of Service (DDoS) Attack Detection: A Systematic Literature Review"

[16]. A. Saied et. al. (2016). "Detection of Known and Unknown DDoS Attacks Using Artificial

Neural Networks," Neurocomputing, vol. 172, pp. 385–93.

[17]. Rupesh Kamble, Hitesh Nemade, Manoj Ghodekar, Rina Waghmode: "Defense Mechanism For Ddos Attack Through Machine Learning", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[18]. F. Fang et. al. (2015). "When Security Games Go Green: Designing Defender Strategies to Prevent Poaching and Illegal Fish- ing," Proc. Int'l. Joint Conf. Artificial Intelligence, pp. 2589–95.

[19]. A. Sinha et. al. (2016). "Learning Adversary Behavior in Security Games: A PAC Model Perspective," Proc. 2016 Int'l. Conf. Autonomous Agents & Multivalent Systems, Richland, SC, 2016, pp. 214–22.

[20]. K. K. Trejo et. al. (2018). "Adapting Attackers and Defenders Patrolling Strategies: A Reinforcement Learning Approach for Stackelberg Security Games," J. Computer and System Sciences, vol. 95, no. 99, 2018, pp. 35–54.

[21]. A. Stavro et. al. (2016). "On the Move: Evading Distributed Deni- al-of-Service Attacks," IEEE Computer, Vol. 49, No. 3, pp. 104–07.

[22]. Jia Q et. al. (2014). "Catch Me if You Can: A Cloud-Enabled DDoS Defense," IEEE/IFIP Int'l. Conf. Dependable Systems and Networks, pp. 264–75.

[23]. M. Albanese et. al. (2018). "Defending from Stealthy Botnets Using Moving Target Defenses," IEEE Security & Privacy, vol. 16, no. 1, 2018, pp. 92–97.

Corresponding Author

Bhargava R.*

PhD Student, Kalinga University, Raipur