JAMM

Journal of Artificial Intelligence and Machine Learning in Management

Open Access

ACM classification:
Security and Privacy → Denial-of-service attacks;
Security and Privacy → Distributed systems security;
Security and Privacy → Network security;
Information Systems → Enterprise systems;
Information Systems → Security.

DDoS Defense Systems in Large Enterprises: A Comprehensive Review of Adoption, Challenges, and Strategies

Chenglin Liu
https://orcid.org/0009-0005-6781-3713

Jia Huang
https://orcid.org/0009-0006-0451-318X

RECEIVED
17 May 2017

REVISED
6 December 2017

ACCEPTED FOR PUBLICATION
8 January 2018
PUBLISHED
14 January 2018

Keywords:
Control structure, Defense location, DDoS attacks, Infrastructure-based defense, Large enterprises, Layered defense approach, Misuse detection technique

Abstract

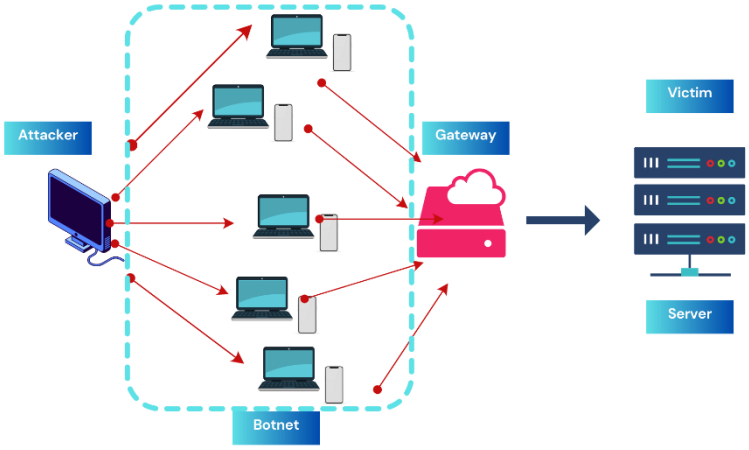
This research aims to review and discuss the adoption, challenges, and strategies of large enterprises regarding five categories related to DDoS attacks: approaches to confronting DDoS attacks, control structure used to counterattack traffic, infrastructure-based DDoS defense, based on defense location, and based on technique used. The findings of this study provide insights into the strategies that large enterprises can adopt to overcome the challenges and provide effective protection against DDoS attacks. Regarding approaches to confronting DDoS attacks, large enterprises need to adopt a multi-layered approach that includes investing in advanced hardware and software capabilities, implementing a threat intelligence program, and adopting a proactive approach to testing and improvement. This approach can help prevent DDoS attacks and mitigate their impact. In terms of control structure used to counterattack traffic, three types were discussed: centralized, hierarchical, and distributed DDoS defense. Each type presents challenges, but careful planning and execution, along with the adoption of best practices, can ensure the security and stability of enterprise networks. Infrastructure-based DDoS defense was also analyzed, with two types discussed: host-based and network-based DDoS defense. Enterprises need to adopt a layered approach, employing automation and orchestration tools, and employing continuous monitoring and threat intelligence to ensure effective defense against DDoS attacks. Based on defense location, three types were discussed: victim-end, intermediate network, and source-end DDoS defense. The study recommends that enterprises adopt a layered defense approach, implement network segmentation, zero-trust security, and use advanced technologies like machine learning to ensure effective protection against DDoS attacks. The study also discussed the misuse detection technique, which is used to prevent DDoS attacks by investing in hardware-based systems and updating rule sets regularly to adapt to new attack patterns. Enterprises need to implement a layered defense approach that includes both misuse and anomaly detection techniques and cloud-based DDoS protection services to provide cost savings and faster response times.

Introduction

In recent years, DDoS attacks have become increasingly common, with a growing number of high-profile attacks affecting businesses and organizations of all sizes. Distributed Denial of Service (DDoS) attacks are a type of cyber attack that aim to disrupt the availability of a targeted system or network [1]. In a DDoS attack, multiple compromised devices, often referred to as a botnet, are used to flood the target with a high volume of traffic or requests, overwhelming the system and causing it to become unavailable to legitimate users as depicted in figure 1. These attacks are often carried out by malicious actors seeking to disrupt services or extort money from their victims.

DDoS attacks are typically categorized based on the type of traffic used to flood the target. For example, network layer attacks involve overwhelming the target's network infrastructure with a high volume of traffic, while application layer attacks target the web application or service itself by exploiting vulnerabilities or overwhelming it with requests. Another common type of DDoS attack is a protocol attack, which aims to flood the target with malformed packets or other malicious traffic that exploit vulnerabilities in the targeted system's protocols [2].

Figure 1. Diagram depicting a DDoS attack



The impact of DDoS attacks can vary depending on the target and the severity of the attack. In some cases, the target may become completely unavailable to legitimate users, causing significant disruption to businesses or individuals. This can result in lost revenue, damage to reputation, and even legal action in some cases. In addition, DDoS attacks can be used as a smokescreen for other cyber attacks, such as data theft or malware installation, further increasing their potential impact.

There are several factors contributing to this trend, including the increasing availability of tools and services that make it easier for attackers to launch DDoS attacks, as well as the growing number of internet-connected devices that can be compromised and used as part of a botnet. One of the primary drivers of the rise in DDoS attacks is the increasing availability of attack tools and services on the dark web. These tools and services allow attackers to launch sophisticated and powerful attacks with minimal effort and expertise, making it easier for even amateur hackers to carry out large-scale attacks. Additionally, many of these tools and services are offered as a subscription service, making it possible for attackers to launch repeated attacks

over a long period of time. Another contributing factor to the rise in DDoS attacks is the growing number of internet-connected devices that can be compromised and used as part of a botnet. With the increasing popularity of the Internet of Things (IoT), there are now billions of connected devices, many of which are poorly secured and vulnerable to attack. This has created a large pool of potential botnet devices that attackers can use to launch DDoS attacks, amplifying their impact and making it more difficult to mitigate them [3].

The rise in DDoS attacks is also fueled by the increasing use of these attacks as a tool for political activism or cybercrime. In some cases, attackers may launch DDoS attacks to disrupt the operations of a business or organization as part of a political or social protest. In other cases, attackers may use DDoS attacks as a smokescreen to distract defenders while they carry out other cyber attacks, such as data theft or ransomware installation. As the use of DDoS attacks becomes more widespread, it is likely that we will continue to see an increase in the frequency and severity of these attacks in the coming years.

DDoS defense system in large enterprises based on approaches to confronting attacks

Intrusion defense systems large enterprises can be categorized into four types based on their approach to confronting DDoS attacks as presented in table 1.

Table 1. Approaches to confronting DDoS attacks

Type of IDS	Approach	Technique
DDoS Detection	Identifying and isolating malicious traffic	Anomaly detection, packet analysis, signature-based detection
DDoS Prevention	Blocking malicious traffic before it reaches the network	Rate limiting, access control, filtering
DDoS Response	Responding to DDoS attacks as they occur	Traffic shaping, packet filtering, rerouting
DDoS Tolerance	Designing the network infrastructure to tolerate DDoS attacks	Load balancing, redundancy, server clustering

The first type is DDoS detection. As the name suggests, this type of defense system is focused on detecting DDoS attacks as soon as they occur. It employs various techniques such as anomaly detection, packet analysis, and signature-based detection to identify and isolate malicious traffic. Once the attack is detected, the system can alert network administrators, who can then take appropriate action to mitigate the attack. The second type is DDoS prevention. This type of defense system is designed to prevent DDoS attacks from ever reaching their target. It uses various techniques such as rate limiting, access control, and filtering to block malicious traffic before it can reach the network [4]. DDoS prevention systems are highly effective in stopping attacks before they can cause any damage, but they can also block legitimate traffic if they are not configured properly. Therefore, it is crucial to ensure that the system is set up correctly to prevent false positives.

The third type is DDoS response. This type of defense system is focused on responding to DDoS attacks as they occur. It uses various techniques such as traffic shaping, packet filtering, and rerouting to manage the network traffic during an attack. DDoS response systems are effective in mitigating the impact of an attack, but they can also be resource-intensive and require careful planning to ensure that they do not cause any disruption to legitimate network traffic. The fourth type is DDoS tolerance. This type of defense system is focused on designing

the network infrastructure in a way that can tolerate DDoS attacks without being affected. DDoS tolerance systems can include techniques such as load balancing, redundancy, and server clustering to ensure that the network can continue to function even under attack. However, DDoS tolerance systems are generally more expensive and complex to implement than other types of defense systems.

i. DDoS Detection

DDoS detection is focused on identifying and isolating malicious traffic as soon as it occurs. Large enterprises that rely on their network for their daily operations must have a robust DDoS detection system in place to protect their data and reputation. The adoption of this type of system by large enterprises has increased over the years due to the rising number and sophistication of DDoS attacks. . One of the main challenges is the complexity of the system itself. It requires advanced knowledge of network architecture, protocols, and security measures to implement and maintain [5]. Additionally, detecting DDoS attacks can be challenging as the attacks can be launched from multiple sources and can mimic legitimate traffic. Therefore, it is crucial to ensure that the detection system is configured correctly and regularly updated with the latest threat intelligence to identify new and emerging threats.

Large enterprises can adopt various strategies when implementing a DDoS detection system. Firstly, they can conduct a thorough risk assessment to identify potential vulnerabilities in their network and determine the level of protection required. Secondly, they can invest in skilled personnel who can manage and maintain the detection system, ensuring that it is always up-to-date and effective. Thirdly, they can adopt a multi-layered approach that combines DDoS detection with other security measures such as firewalls, intrusion prevention systems, and user behavior analytics to provide comprehensive protection against cyber threats.

Moreover, large enterprises can leverage cloud-based DDoS detection services. These services can provide scalable and cost-effective solutions that can quickly detect and mitigate DDoS attacks. Additionally, they can be integrated with existing security infrastructure, reducing the complexity of managing a separate detection system. However, it is important to ensure that the service provider has a robust and reliable infrastructure and offers high-quality support to minimize any potential downtime or disruption to the enterprise's network. Large enterprises can adopt a proactive approach to DDoS detection by regularly testing their systems and simulating attacks. This can help identify any weaknesses or gaps in the system and provide an opportunity to improve and fine-tune the detection capabilities. It can also provide valuable insights into the effectiveness of the overall security posture and highlight any areas that require further attention. Implementing a DDoS detection system is a critical step for large enterprises to protect their network and data from cyber threats. However, it comes with its challenges, and adopting the right strategies can help overcome these challenges and provide effective protection against DDoS attacks. These strategies include conducting a thorough risk assessment, investing in skilled personnel, adopting a multi-layered approach, leveraging cloud-based services, and adopting a proactive approach to testing and improvement.

ii. DDoS Prevention

DDoS prevention focuses on blocking malicious traffic before it reaches the network. This type of system is essential for large enterprises that require high availability and uptime of their network infrastructure. By blocking malicious traffic, DDoS prevention systems can prevent disruption to legitimate traffic and ensure that critical services remain available. One of the primary challenges of DDoS prevention systems is the potential for false positives, which can result in legitimate traffic being blocked. This can cause significant disruptions to business

operations and potentially result in lost revenue. Therefore, it is essential to ensure that the DDoS prevention system is configured correctly and regularly updated with the latest threat intelligence to minimize the risk of false positives. Another challenge of DDoS prevention systems is that they require significant resources, both in terms of hardware and personnel. To effectively prevent DDoS attacks, the system must be able to handle large volumes of traffic and be able to distinguish between legitimate and malicious traffic. This requires advanced hardware and software capabilities, as well as skilled personnel to manage and maintain the system.

Large enterprises can adopt various strategies when implementing a DDoS prevention system. Firstly, they can invest in advanced hardware and software capabilities that are specifically designed to handle large volumes of traffic and detect and prevent DDoS attacks. Additionally, they can adopt a multi-layered approach that combines DDoS prevention with other security measures such as firewalls, intrusion prevention systems, and user behavior analytics to provide comprehensive protection against cyber threats [6].

Another strategy that large enterprises can adopt is to implement a threat intelligence program that continuously monitors and updates the DDoS prevention system with the latest threat intelligence. This can help identify new and emerging threats and ensure that the prevention system is always up-to-date and effective in blocking malicious traffic.

Finally, large enterprises can adopt a proactive approach to DDoS prevention by regularly testing their systems and simulating attacks. This can help identify any weaknesses or gaps in the system and provide an opportunity to improve and fine-tune the prevention capabilities. It can also provide valuable insights into the effectiveness of the overall security posture and highlight any areas that require further attention.

iii. DDoS Response

DDoS response is the third type of intrusion defense system that focuses on mitigating the impact of a DDoS attack once it has already started. This type of system is critical for large enterprises that may face a DDoS attack despite having prevention systems in place. A DDoS response system can help reduce the impact of the attack and minimize the disruption to business operations. However, implementing a DDoS response system comes with its own set of challenges.

One of the primary challenges of DDoS response systems is the ability to detect and respond to DDoS attacks quickly. DDoS attacks can quickly overwhelm a network, and a slow response time can result in significant disruption and damage to business operations. Therefore, it is essential to have a robust response plan in place and to regularly test and update the plan to ensure that it is effective.

Another challenge of DDoS response systems is the potential for false positives, which can result in legitimate traffic being blocked. This can cause significant disruptions to business operations and potentially result in lost revenue. Therefore, it is essential to ensure that the DDoS response system is configured correctly and regularly updated with the latest threat intelligence to minimize the risk of false positives. Large enterprises can adopt various strategies when implementing a DDoS response system. Firstly, they can invest in advanced hardware and software capabilities that are specifically designed to detect and respond to DDoS attacks quickly and efficiently. Additionally, they can implement a comprehensive response plan that includes procedures for detecting, isolating, and mitigating the impact of a DDoS attack.

Another strategy that large enterprises can adopt is to implement a threat intelligence program that continuously monitors and updates the DDoS response system with the latest threat intelligence. This can help identify new and emerging threats and ensure that the response system is always up-to-date and effective in mitigating the impact of a DDoS attack.

Finally, large enterprises can adopt a proactive approach to DDoS response by regularly testing their systems and simulating attacks. This can help identify any weaknesses or gaps in the system and provide an opportunity to improve and fine-tune the response capabilities. It can also provide valuable insights into the effectiveness of the overall security posture and highlight any areas that require further attention.

iv. DDoS Tolerance

DDoS tolerance is the fourth type of intrusion defense system, which focuses on minimizing the impact of DDoS attacks by ensuring that critical services remain available despite the attack. This approach is particularly useful for large enterprises that cannot afford to have their services disrupted, even for a short period. DDoS tolerance systems allow organizations to continue operating during an attack, which can significantly reduce the impact of the attack on business operations.

One of the primary challenges of implementing a DDoS tolerance system is the cost associated with it. DDoS tolerance systems require redundancy and backup infrastructure, which can be costly to implement and maintain. Additionally, DDoS tolerance systems may require more significant investments in hardware and software to ensure that critical services can continue to function during an attack.

Another challenge of DDoS tolerance systems is the complexity of managing and maintaining redundant infrastructure. This requires additional resources and expertise, which may not be available to all organizations. Therefore, it is essential to ensure that the organization has the necessary resources and expertise to manage and maintain a DDoS tolerance system effectively. Large enterprises can adopt various strategies when implementing a DDoS tolerance system. Firstly, they can prioritize critical services and infrastructure that require protection from DDoS attacks. This can help identify the areas where redundancy and backup infrastructure are needed the most, and focus resources and investments accordingly.

Secondly, large enterprises can adopt a cloud-based approach to DDoS tolerance, which can reduce the cost and complexity of implementing and maintaining a DDoS tolerance system. Cloud-based solutions can provide scalable and flexible infrastructure that can be quickly deployed and managed, reducing the time and resources required to implement a DDoS tolerance system. Another strategy that large enterprises can adopt is to implement a comprehensive disaster recovery plan that includes procedures for maintaining critical services during a DDoS attack [6]. This can help ensure that the organization is prepared for an attack and can quickly and efficiently respond to minimize the impact on business operations.

Large enterprises can adopt a proactive approach to DDoS tolerance by regularly testing their systems and simulating attacks. This can help identify any weaknesses or gaps in the system and provide an opportunity to improve and fine-tune the tolerance capabilities. It can also provide valuable insights into the effectiveness of the overall security posture and highlight any areas that require further attention.

Table 2. Challenges and strategies in approaches to confronting DDoS attacks

Type	Focus	Challenges	Strategies
DDoS Detection	Identifying and isolating malicious traffic	Complexity of the system, challenging to detect DDoS attacks	Conducting a thorough risk assessment, investing in skilled personnel, adopting a multi-layered approach, leveraging cloud-based services, and adopting a proactive approach to testing and improvement
DDoS Prevention	Blocking malicious traffic before it reaches the network	Potential for false positives, requires significant resources	Investing in advanced hardware and software capabilities, adopting a multi-layered approach, implementing a threat intelligence program, and adopting a proactive approach to testing and improvement
DDoS Response	Mitigating the impact of a DDoS attack once it has already started	Challenges not mentioned	Monitoring the network and traffic, isolating the attack, mitigating the impact, and implementing a disaster recovery plan

DDoS defense system in large enterprises-based on control structure used to counterattack traffic

There are several types of DDoS defense systems, based on the control structure used to counterattack traffic. One approach is centralized defense, which involves routing all traffic through a single location, such as a network operations center (NOC) or a security operations center (SOC), where it can be monitored and analyzed for signs of an attack. If an attack is detected, the centralized system can initiate countermeasures, such as blocking or rate-limiting traffic from suspicious sources.

Another approach to DDoS defense is hierarchical, which involves using multiple layers of defense distributed across the network. In a hierarchical defense system, traffic is first filtered at the network edge by firewalls and intrusion prevention systems (IPS), which block traffic from known bad actors and apply policies to limit traffic from other sources. Next, traffic is analyzed by a middle layer of security devices, such as load balancers or DDoS mitigation appliances, which use advanced techniques to detect and mitigate DDoS attacks. If an attack is detected, the traffic is routed to a centralized scrubbing center, where it can be further analyzed and filtered before being allowed to reach the target system [7].

Table 3. control structure used to counterattack traffic

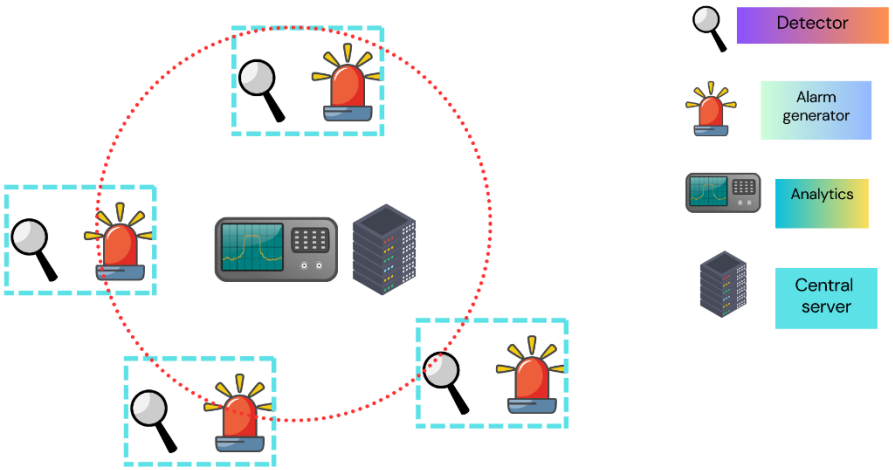
Control Structure	Description
Centralized	All traffic is routed through a single location, such as a NOC or SOC, where it can be monitored and analyzed for signs of an attack. If an attack is detected, the centralized system can initiate countermeasures, such as blocking or rate-limiting traffic from suspicious sources.
Hierarchical	Multiple layers of defense are distributed across the network, with each layer performing a specific function such as filtering, analysis, or mitigation. Traffic is first filtered at the network edge by firewalls and IPS, then analyzed by middle layer devices such as load balancers or DDoS mitigation appliances. Finally, if an attack is detected, the traffic is routed to a centralized scrubbing center.
Distributed	Uses a decentralized network of sensors and mitigation devices to detect and mitigate attacks in real-time. Each sensor monitors a portion of the network for signs of an attack, and can autonomously initiate countermeasures. Sensors can communicate with each other to share information about the attack, allowing the system to respond quickly and effectively.

A third approach to DDoS defense is distributed, which involves using a decentralized network of sensors and mitigation devices to detect and mitigate attacks in real-time. In a distributed defense system, each sensor monitors a portion of the network for signs of an attack, and can autonomously initiate countermeasures, such as blocking or rate-limiting traffic from suspicious sources. The sensors can also communicate with each other to share information about the attack, allowing the system to respond more effectively and quickly. This approach is particularly effective against attacks that are highly distributed and difficult to detect using traditional centralized or hierarchical defenses.

i. Centralized DDoS Defense

Large enterprises have increasingly adopted centralized DDoS defense systems to protect their networks and infrastructure from the growing threat of DDoS attacks. One of the main reasons for this adoption is the ease of management and control offered by centralized systems, which allow for a unified and consistent approach to DDoS detection and prevention. Centralized systems can also leverage advanced analytics and machine learning to detect and mitigate attacks, making them more effective and efficient than traditional manual approaches [8].

Figure 2. Centralized DDoS Defense



However, there are several challenges that large enterprises face when implementing centralized DDoS defense systems. One of the biggest challenges is the risk of a single point of failure, as all traffic must pass through a single location, such as a NOC or SOC. If the centralized system is overwhelmed by an attack, the entire network can be disrupted, leading to significant downtime and loss of revenue. To mitigate this risk, large enterprises must invest in redundant and resilient infrastructure, such as multiple NOCs or SOC, to ensure continuity of service in the event of an attack [9-11].

Additionally, there is the potential for increased network latency or disruptions, as all traffic must pass through the centralized system. This can be particularly problematic for large enterprises that rely on low-latency connections for critical applications, such as financial trading or online gaming. To address this challenge, large enterprises must carefully design

their centralized defense systems to minimize latency and disruption, while still maintaining a high level of security.

Large enterprises can also face challenges in scaling their centralized DDoS defense systems to handle increasing traffic volumes and attack intensity. As DDoS attacks become more sophisticated and powerful, centralized systems must be able to scale up quickly to handle the increased demand. This requires a significant investment in hardware and software, as well as skilled personnel to manage and maintain the systems. Enterprises can adopt several strategies for implementing centralized DDoS defense systems. These strategies include:

1. Redundancy and Resilience: Deploying multiple NOCs or SOC to ensure continuity of service in the event of an attack.
2. Advanced Analytics and Machine Learning: Leveraging advanced analytics and machine learning to detect and mitigate attacks, improving the efficiency and effectiveness of the defense system.
3. Multi-Layered Defense: Implementing a multi-layered defense approach, such as hierarchical, to provide multiple layers of defense distributed across the network.
4. Scalability: Investing in hardware and software to scale the centralized system quickly to handle increasing traffic volumes and attack intensity.

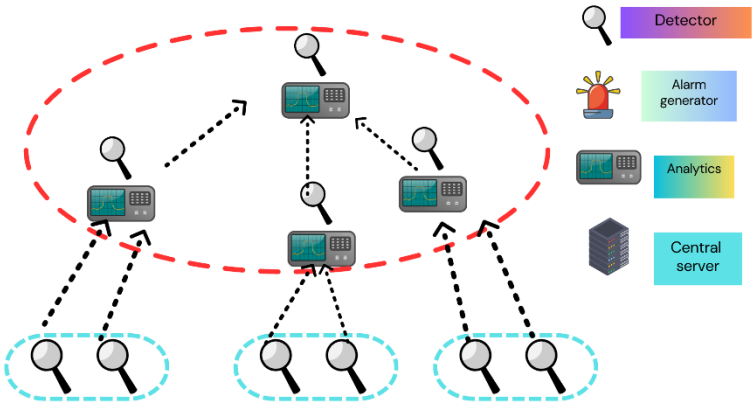
ii. Hierarchical DDoS Defense

The hierarchical DDoS defense system is another popular approach that large enterprises have adopted to protect their networks from DDoS attacks. This type of system involves distributing multiple layers of defense across the network, with each layer performing a specific function such as filtering, analysis, or mitigation. Traffic is first filtered at the network edge by firewalls and IPS, then analyzed by middle layer devices such as load balancers or DDoS mitigation appliances. Finally, if an attack is detected, the traffic is routed to a centralized scrubbing center for further analysis and mitigation. One of the main advantages of the hierarchical approach is its comprehensive approach to DDoS defense. By using multiple layers of defense distributed across the network, this approach can effectively detect and mitigate both low and high-intensity DDoS attacks [12-14]. Additionally, the distributed nature of this approach makes it less vulnerable to single points of failure, as each layer can continue to function even if another layer is compromised.

However, implementing a hierarchical DDoS defense system can be complex and challenging for large enterprises. One of the main challenges is the significant investment in hardware and software required to set up and maintain the system. This includes deploying multiple layers of defense, such as firewalls, IPS, load balancers, and DDoS mitigation appliances, and the skilled personnel to manage and maintain these devices. Another challenge is the potential for increased network latency and disruption, as traffic is routed through multiple layers of defense. This can be particularly problematic for large enterprises that rely on low-latency connections for critical applications. To address this challenge, large enterprises must carefully design their hierarchical defense systems to minimize latency and disruption while still maintaining a high level of security.

The strategies include investing in redundant and resilient infrastructure to ensure continuity of service in the event of an attack, leveraging automation and orchestration to simplify the management of multiple layers of defense, and deploying advanced analytics and machine learning to improve the efficiency and effectiveness of the defense system.

Figure 2. Hierarchical DDoS Defense



In addition, large enterprises can benefit from collaborating with industry peers and security experts to share information and best practices. This can help to improve the overall effectiveness of the hierarchical defense system and ensure that it is up-to-date with the latest DDoS attack trends and techniques.

iii. Distributed DDoS Defense

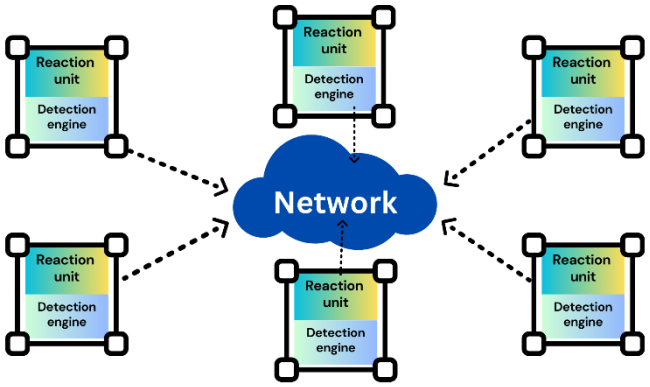
The distributed DDoS defense system is a unique approach that involves leveraging the power of distributed networks to defend against DDoS attacks. In this type of system, multiple geographically dispersed nodes work together to detect and mitigate DDoS attacks in real-time. Each node operates independently but communicates with other nodes in the network to share threat intelligence and coordinate defense activities. One of the main advantages of the distributed approach is its scalability and flexibility [15]. Because the defense system is distributed across multiple nodes, it can easily scale up or down as needed to handle changes in network traffic and attack volumes. Additionally, the distributed nature of the system makes it highly resilient and less vulnerable to single points of failure, as each node can continue to operate even if other nodes are compromised [16].

However, implementing a distributed DDoS defense system can be challenging for large enterprises. One of the main challenges is ensuring that all nodes in the network are properly configured and maintained to ensure optimal performance and security. This requires a significant investment in hardware, software, and skilled personnel to manage and maintain the distributed nodes.

Another challenge is the potential for increased network latency and disruption, as traffic is routed through multiple nodes in the network. To address this challenge, large enterprises must carefully design their distributed defense systems to minimize latency and disruption while still maintaining a high level of security. Enterprises can adopt several strategies for implementing distributed DDoS defense systems. These strategies include deploying advanced analytics and

machine learning to enable real-time threat detection and mitigation, leveraging automation and orchestration to simplify the management of distributed nodes, and collaborating with industry peers and security experts to share information and best practices [17].

Figure 3. Distributed DDoS Defense



DDoS defense system in large enterprises based on infrastructure

To protect against DDoS attacks, various defense systems have been developed based on the infrastructure used. Two basic types of DDoS defense systems are host-based and network-based defense. Host-based DDoS defense involves installing software or hardware on individual hosts or servers to detect and mitigate DDoS attacks. Host-based defense systems can quickly detect attacks and mitigate them before they cause significant damage. These systems work by analyzing incoming traffic, detecting patterns that are indicative of a DDoS attack, and then filtering out the malicious traffic. One drawback of host-based defense is that it can be resource-intensive and may slow down the performance of the host.

Network-based DDoS defense, on the other hand, involves deploying hardware or software on network devices such as routers, switches, or firewalls to detect and mitigate DDoS attacks. This approach provides protection for an entire network and can quickly detect and mitigate attacks. Network-based defense systems work by analyzing traffic patterns across the network, identifying and blocking malicious traffic. One benefit of network-based defense is that it can be less resource-intensive than host-based defense, but it may not be as effective in detecting and mitigating attacks on individual hosts [18].

Host-Based DDoS Defense

Host-based DDoS defense is an essential cybersecurity strategy that large enterprises employ to protect their critical systems and assets. Host-based defense is a proactive approach that involves deploying software or hardware on individual hosts or servers to detect and mitigate DDoS attacks. The adoption of host-based defense by large enterprises is crucial in the face of the ever-increasing threat landscape of DDoS attacks. One of the main challenges is the resource-intensive nature of host-based defense. Large enterprises may have a vast number of hosts and servers, which makes it challenging to deploy and manage host-based defense systems. Moreover, host-based defense systems can slow down the performance of hosts, leading to reduced productivity and user experience. Organizations employ various strategies

to ensure effective host-based DDoS defense. One strategy is to deploy host-based defense systems in a layered approach, where multiple systems are deployed at different levels of the network infrastructure. This approach ensures that attacks are detected and mitigated at multiple levels, thereby reducing the likelihood of a successful attack [19-21].

Another strategy is to employ automation and orchestration tools to streamline the deployment and management of host-based defense systems. These tools enable enterprises to automate the detection and mitigation of DDoS attacks, thereby reducing the workload on security teams. Additionally, automation tools can quickly identify new attack patterns and update defense systems in real-time, ensuring that enterprises are protected against the latest threats.

Large enterprises also employ continuous monitoring and threat intelligence to stay ahead of DDoS attacks. Continuous monitoring ensures that any suspicious activity is detected and analyzed in real-time, allowing for quick mitigation of attacks. Threat intelligence provides valuable insights into the latest attack trends, enabling enterprises to prepare and respond appropriately. The adoption of host-based DDoS defense by large enterprises is crucial to protect against the ever-increasing threat landscape of DDoS attacks. While there are challenges to deploying and managing host-based defense systems, enterprises can employ various strategies to overcome these challenges and ensure effective defense. By adopting a layered approach, employing automation and orchestration tools, and employing continuous monitoring and threat intelligence, large enterprises can stay ahead of DDoS attacks and protect their critical systems and assets [22-25].

Network-Based DDoS Defense

Network-based DDoS defense is another critical cybersecurity strategy that large enterprises employ to protect their networks from DDoS attacks. Network-based defense involves deploying hardware or software on network devices such as routers, switches, or firewalls to detect and mitigate DDoS attacks. The adoption of network-based defense by large enterprises is crucial to protect against attacks that target the entire network infrastructure.

However, the adoption of network-based DDoS defense also comes with its own set of challenges. One of the main challenges is the cost of deploying and maintaining network-based defense systems. Large enterprises may need to invest in expensive hardware and software solutions to ensure adequate protection. Moreover, network-based defense systems can be complex to deploy and manage, requiring highly skilled security personnel. One strategy is to employ cloud-based DDoS protection services, which offer a cost-effective solution to protect against DDoS attacks. Cloud-based DDoS protection services allow enterprises to outsource the deployment and management of network-based defense systems to a third-party provider, thereby reducing the workload on internal security teams. Another strategy is to employ machine learning and artificial intelligence (AI) to enhance the effectiveness of network-based defense systems. Machine learning and AI can quickly analyze vast amounts of data to detect and mitigate DDoS attacks in real-time. By using these technologies, enterprises can stay ahead of the latest attack trends and ensure effective defense against DDoS attacks.

Large enterprises also employ threat intelligence and collaboration with other organizations to enhance their network-based DDoS defense. Threat intelligence provides valuable insights into the latest attack trends, enabling enterprises to prepare and respond appropriately. Collaboration with other organizations allows enterprises to share information and best practices, enabling them to stay ahead of DDoS attacks and improve their defense posture. The adoption of network-based DDoS defense by large enterprises is crucial to protect against attacks that target the entire network infrastructure. While there are challenges to deploying and managing

network-based defense systems, enterprises can employ various strategies to overcome these challenges and ensure effective defense. By employing cloud-based DDoS protection services, machine learning and AI, threat intelligence, and collaboration with other organizations, large enterprises can protect their networks against DDoS attacks and ensure business continuity [26-29].

Table 4. DDoS defense system in large enterprises based on infrastructure

	Host-Based DDoS Defense	Network-Based DDoS Defense
Approach	Deploys software/hardware on individual hosts or servers to detect and mitigate DDoS attacks	Deploys hardware/software on network devices (routers, switches, firewalls) to detect and mitigate DDoS attacks targeting the entire network infrastructure
Challenges	Resource-intensive and may slow down host performance, challenging to deploy and manage on large enterprise systems	Expensive to deploy and maintain, complex to deploy and manage, requiring highly skilled security personnel
Strategies	Layered approach, automation and orchestration tools, continuous monitoring, and threat intelligence	Cloud-based DDoS protection services, machine learning and AI, threat intelligence, and collaboration with other organizations
Benefits	Reduces the likelihood of a successful attack, detects new attack patterns in real-time, and protects critical systems and assets	Offers cost-effective solutions, detects and mitigates attacks in real-time, and enhances defense effectiveness through machine learning and AI
Overall Goal	To protect critical systems and assets from DDoS attacks	To protect the entire network infrastructure from DDoS attacks

DDoS defense system in large enterprises based on defense location

Organizations can deploy a DDoS defense system in three possible locations: victim end, intermediate, and source end. The choice of deployment location depends on the organization's resources, network architecture, and specific security requirements.

Table 5. Deployment locations for DDoS defense systems

Deployment Location	Description
Victim End	A DDoS defense system placed at the victim end is located at the network edge or directly in front of the targeted servers. This approach allows the system to identify and block malicious traffic before it reaches the target servers.
Intermediate	A DDoS defense system placed at the intermediate location is located in a cloud-based or third-party network provider's network. This approach enables organizations to mitigate DDoS attacks at the network edge without investing in expensive infrastructure. A cloud-based mitigation system can handle high-capacity attacks and provide near real-time traffic analysis.
Source End	A DDoS defense system placed at the source end is located in the network that connects the organization to the internet. This approach enables the system to identify and block malicious traffic before it enters the organization's network. However, implementing this approach can be challenging as it requires cooperation from upstream providers and may not be effective against attacks that originate from multiple sources.

Deploying a DDoS defense system at the victim end involves placing a mitigation system at the organization's network edge or directly in front of the targeted servers. This approach enables the system to identify and block malicious traffic before it reaches the target servers. However, this approach can be expensive as it requires high-capacity mitigation systems and may not be effective against sophisticated attacks.

Deploying a DDoS defense system at the intermediate location involves placing the mitigation system in a cloud-based or third-party network provider's network. This approach allows organizations to mitigate DDoS attacks at the network edge without having to invest in expensive infrastructure [31]. Moreover, a cloud-based mitigation system can handle high-capacity attacks and provide near real-time traffic analysis [32].

Deploying a DDoS defense system at the source end involves placing the mitigation system in the network that connects the organization to the internet. This approach enables the system to identify and block malicious traffic before it enters the organization's network [33]. However, this approach can be challenging to implement as it requires cooperation from upstream providers and may not be effective against attacks that originate from multiple sources.

Victim-End DDoS Defense

Adopting a DDoS defense system at the victim end is a popular strategy for large enterprises to protect their networks from cyber attacks. This approach involves deploying the mitigation system directly in front of the targeted servers or at the network edge to detect and block malicious traffic before it reaches the servers. While this strategy is effective, it can also present challenges for large enterprises. One of the main challenges of adopting a DDoS defense system at the victim end is the cost of deploying and maintaining the infrastructure. Large enterprises must invest in high-capacity mitigation systems capable of handling large-scale DDoS attacks, which can be expensive [34]. Additionally, they must allocate resources to maintain and update the system to ensure its effectiveness.

Another challenge is the possibility of false positives, where legitimate traffic is identified as malicious and blocked by the mitigation system. This can disrupt the organization's operations and lead to loss of revenue. To address this, large enterprises must continuously monitor and tune their DDoS defense systems to minimize the occurrence of false positives. One technique is to work with a specialized security vendor that can provide expertise and support in deploying and maintaining the system. This can help to reduce costs and ensure that the system is optimized for the organization's specific needs. Another strategy is to implement a multi-layered defense approach that includes not only a DDoS defense system but also other security measures such as firewalls, intrusion prevention systems, and threat intelligence feeds. This can help to reduce the risk of a successful attack and improve the overall security posture of the organization [35]. They can use cloud-based mitigation services that offer scalable and cost-effective solutions. These services can provide real-time traffic analysis and reduce the need for expensive infrastructure investments. However, organizations must ensure that the cloud-based solution is compatible with their existing network architecture and meets their specific security requirements. Adopting a DDoS defense system at the victim end is a critical strategy for large enterprises to protect their networks from cyber attacks. While it presents challenges, implementing the right strategies and partnering with the right security vendors can help to mitigate these challenges and provide effective protection against DDoS attacks.

Intermediate Network DDoS Defense

Deploying a DDoS defense system at the intermediate location is another popular strategy for large enterprises to protect their networks from DDoS attacks. This approach involves placing

the mitigation system in a cloud-based or third-party network provider's network to mitigate DDoS attacks at the network edge without investing in expensive infrastructure.

One of the challenges of adopting a DDoS defense system at the intermediate location is the need to ensure compatibility with the organization's existing network architecture. The cloud-based solution must integrate seamlessly with the organization's network and provide effective protection against DDoS attacks.

Another challenge is ensuring the security and reliability of the cloud-based solution. Organizations must carefully evaluate the security and reliability of the cloud provider, including their security policies, procedures, and certifications. Additionally, they must ensure that the provider can handle high-capacity attacks and provide real-time traffic analysis. Organizations can employ several strategies when deploying a DDoS defense system at the intermediate location. One strategy is to work with a trusted and reliable cloud provider that has a proven track record in providing effective DDoS mitigation solutions. Organizations must also conduct regular audits and assessments of the cloud provider's security and reliability. Another strategy is to implement a hybrid defense approach that combines on-premise and cloud-based solutions. This can provide organizations with greater flexibility and control over their DDoS defense systems while leveraging the scalability and cost-effectiveness of cloud-based solutions.

In addition, organizations can use machine learning and artificial intelligence (AI) to improve their DDoS defense systems' effectiveness. Machine learning and AI can enable organizations to detect and block sophisticated DDoS attacks in real-time, improving the overall security posture of the organization. Deploying a DDoS defense system at the intermediate location can provide large enterprises with effective protection against DDoS attacks while reducing the need for expensive infrastructure investments. By implementing the right strategies and working with trusted and reliable cloud providers, organizations can overcome the challenges associated with this approach and improve their overall security posture.

Source-End DDoS Defense

Deploying a DDoS defense system at the source end is a proactive strategy for large enterprises to prevent DDoS attacks from occurring in the first place. This approach involves identifying and blocking malicious traffic at the source, such as infected devices or botnets, before it reaches the victim network.

One of the challenges of adopting a DDoS defense system at the source end is the complexity of identifying and blocking malicious traffic. This requires real-time monitoring of network traffic and the ability to distinguish legitimate traffic from malicious traffic. Additionally, organizations must identify and block malicious traffic without disrupting legitimate traffic, which can be challenging.

Another challenge is the need to ensure the system's scalability and effectiveness in blocking large-scale DDoS attacks. As the number of devices and endpoints grows, the system must be able to handle the increased traffic and identify and block malicious traffic effectively. One strategy is to implement a network segmentation approach that separates critical assets and applications from the rest of the network. This can help to limit the attack surface and reduce the impact of a successful DDoS attack. Another strategy is to implement a zero-trust security model that assumes all network traffic is potentially malicious. This can help to identify and block malicious traffic at the source while reducing the risk of false positives. In addition, organizations can use threat intelligence feeds and machine learning algorithms to identify and

block malicious traffic in real-time. These technologies can improve the system's effectiveness in identifying and blocking large-scale DDoS attacks.

Deploying a DDoS defense system at the source end is a proactive strategy for large enterprises to prevent DDoS attacks from occurring. While it presents challenges, implementing the right strategies, such as network segmentation, zero-trust security, and using advanced technologies like machine learning, can help to mitigate these challenges and provide effective protection against DDoS attacks.

DDoS defense system in large enterprises based on technique used

Misuse detection and anomaly detection are two techniques used to prevent DDoS attacks. Misuse detection involves identifying known attack patterns and blocking them. This technique uses pre-determined rules to filter out traffic that matches known attack signatures. The downside of this approach is that new, previously unknown attack patterns may still bypass the filters. However, it is an effective technique for detecting well-known attack patterns.

On the other hand, anomaly detection identifies unusual traffic patterns that deviate from normal traffic behavior. Unlike misuse detection, anomaly detection can detect new and unknown attack patterns. The system can learn and adapt to new attacks, making it more effective in identifying and blocking DDoS attacks. However, it may also lead to false positives if the system flags legitimate traffic as anomalous. Anomaly detection requires a high degree of accuracy, and the system needs to learn from past traffic patterns to identify unusual traffic patterns accurately.

Misuse Detection

The adoption of misuse detection techniques by large enterprises has been on the rise due to the increased frequency of DDoS attacks. Enterprises have been investing in hardware-based firewalls and intrusion prevention systems (IPS) to implement misuse detection techniques. These systems use known attack patterns, such as TCP SYN floods and ICMP floods, to detect and block DDoS attacks. While hardware-based systems can provide fast detection and response times, they can be expensive and require a significant amount of maintenance and updates.

One of the challenges of using misuse detection techniques is that attackers can evade detection by modifying their attack patterns. Attackers can use botnets to launch attacks from multiple IP addresses, making it difficult to block traffic that matches known attack patterns. Furthermore, attackers can use legitimate traffic to camouflage their attacks, making it difficult to differentiate between legitimate traffic and malicious traffic. Enterprises need to update their rule sets regularly to adapt to new attack patterns to prevent this evasion.

Enterprises can implement a layered defense approach that includes both misuse and anomaly detection techniques. The layered approach can use hardware-based firewalls and IPS systems to provide fast detection and response times to known attack patterns. In addition, an anomaly detection system can detect new and unknown attack patterns that bypass the misuse detection systems. Enterprises can use machine learning algorithms to train the anomaly detection system to differentiate between normal and abnormal traffic patterns accurately. Another strategy for enterprises is to leverage cloud-based DDoS protection services. Cloud-based DDoS protection services use a network of distributed servers to mitigate DDoS attacks. These services can provide faster detection and response times as they can absorb large volumes of traffic. Cloud-based services can also provide cost savings as enterprises can pay for the services only when

they need them. Enterprises can use cloud-based services in tandem with their hardware-based systems to provide comprehensive DDoS protection.

Large enterprises are adopting misuse detection techniques to prevent DDoS attacks. Enterprises are investing in hardware-based systems and updating their rule sets regularly to adapt to new attack patterns. However, attackers can evade detection by modifying their attack patterns, making it challenging to differentiate between legitimate and malicious traffic. To overcome these challenges, enterprises can implement a layered defense approach that includes both misuse and anomaly detection techniques. Cloud-based DDoS protection services can also provide cost savings and faster response times.

Anomaly Detection

Anomaly detection is another technique used by large enterprises to prevent DDoS attacks. Anomaly detection involves identifying traffic patterns that deviate from normal traffic behavior. Machine learning algorithms are used to train the system to identify unusual traffic patterns that may indicate a DDoS attack. Anomaly detection is effective in identifying new and unknown attack patterns, making it a valuable technique for DDoS defense. One of the challenges of using anomaly detection is the need for a high degree of accuracy. False positives can occur if legitimate traffic is flagged as anomalous, leading to unnecessary traffic filtering and potential service disruptions. To overcome this challenge, enterprises can use a combination of supervised and unsupervised learning techniques to train the system. Supervised learning involves using a training set of labeled data to teach the system what is considered normal traffic behavior. Unsupervised learning involves allowing the system to learn from the data itself to identify unusual traffic patterns. This approach can improve the system's accuracy and reduce the likelihood of false positives.

Table 6. DDoS defense system in large enterprises based on technique used

Technique	Advantages	Challenges	Strategies to overcome challenges
Misuse detection	Fast detection and response times, use of known attack patterns	Attackers can evade detection by modifying attack patterns, difficulty differentiating between legitimate and malicious traffic	Implement a layered defense approach with both misuse and anomaly detection techniques, use cloud-based DDoS protection services
Anomaly detection	Identifies new and unknown attack patterns	Need for high accuracy, need for large amounts of data to train system	Use a combination of supervised and unsupervised learning techniques, use cloud-based services for access to large data sets, use multiple analysis techniques such as flow-based, packet-based, and protocol-based analysis

Additionally, enterprises may struggle to collect enough data to train the system accurately, especially if they have limited resources or if they are dealing with new and unknown attack patterns. To overcome this challenge, enterprises can use cloud-based services that provide access to large data sets. These services can also provide additional resources, such as machine learning experts, to help train the system accurately. To maximize the effectiveness of anomaly detection, enterprises can use a combination of techniques, including flow-based analysis,

packet-based analysis, and protocol-based analysis. Flow-based analysis involves analyzing the flow of traffic between network devices to detect unusual patterns. Packet-based analysis involves analyzing individual packets of data to identify unusual behavior. Protocol-based analysis involves analyzing the behavior of specific network protocols to identify anomalies. By using multiple techniques, enterprises can increase the accuracy of their DDoS defense systems and improve their overall security posture. Anomaly detection is an effective technique for preventing DDoS attacks. Enterprises can use machine learning algorithms to identify unusual traffic patterns and train their systems to detect new and unknown attack patterns. To overcome the challenges of using anomaly detection, enterprises can use a combination of supervised and unsupervised learning techniques, cloud-based services, and multiple analysis techniques. By implementing these strategies, enterprises can enhance their DDoS defense and reduce the risk of service disruptions and potential financial losses.

Conclusion

DDoS attacks can have a significant impact on large enterprises, particularly those that rely heavily on their online presence for business operations. One of the main impacts of DDoS attacks is the disruption of service, which can result in lost revenue, damage to reputation, and decreased customer trust. When a company's website or online service becomes unavailable due to a DDoS attack, customers may turn to competitors or simply give up on attempting to access the service, resulting in a direct financial impact.

In addition to the direct financial impact of DDoS attacks, there can also be indirect costs associated with these attacks. For example, if a company's IT staff must spend significant time and resources responding to a DDoS attack, this can result in delays in other projects or initiatives, as well as increased IT costs. Additionally, the negative publicity and damage to reputation that can result from a successful DDoS attack can have long-term impacts on a company's brand and customer relationships. Another potential impact of DDoS attacks on large enterprises is the potential for these attacks to be used as a smokescreen for other cyber attacks. For example, attackers may launch a DDoS attack on a company's website to distract IT staff while they attempt to steal sensitive data or install malware on the company's systems. In these cases, the impact of the DDoS attack may be only the tip of the iceberg, with more significant damage occurring as a result of the secondary attack.

There are a number of limitations that must be taken into account, despite the fact that this study offers useful insights on the adoption, difficulties, and defense mechanisms used by major businesses against DDoS attacks. Firstly, since the research mainly focuses on big organizations, it can not be generalized to small and medium-sized enterprises. The research only looks at five kinds of DDoS attacks, which means it may not cover all facets of DDoS attack mitigation and prevention. Also, the research mainly depends on literature studies and could not provide a thorough assessment of the present norms and difficulties encountered by big corporations. Nevertheless, the research does not look at the expenses involved in putting different DDoS attack prevention and mitigation measures into practice, which may restrict the viability of certain solutions for smaller businesses. Last but not least, the research excludes the ethical ramifications of using specific DDoS attack prevention and mitigation measures, such the usage of automation and machine learning technologies, which may risk privacy and security. Consequently, these limitations must be taken into account when interpreting the results and extending them to different situations, even though the study's findings provide useful insights into DDoS attack prevention and mitigation measures for big corporations.

References

[1] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "DDoS Incidents and their Impact: A Review," *Int. Arab J. Inf. Technol.*, vol. 7, no. 1, pp. 14–20, 2010.
[2] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, "Research trends in security and DDoS in SDN," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6386–6411, Dec. 2016.
[3] S. Behal and K. Kumar, "Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review," *Int. J. Secur. Netw.*, vol. 19, no. 3, pp. 383–393, 2017.
[4] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp. 147–165, May 2016.
[5] A. Rai and R. K. Challa, "Survey on Recent DDoS Mitigation Techniques and Comparative Analysis," in *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)*, 2016, pp. 96–101.
[6] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surv.*, vol. 39, no. 1, pp. 3-es, Apr. 2007.
[7] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, Fourth 2013.
[8] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242–2270, Fourthquarter 2015.
[9] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 International Conference on Computing, Networking and Communications (ICNC)*, 2015, pp. 77–81.
[10] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016.
[11] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: a classification," in *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795)*, 2003, pp. 190–193.
[12] L. Li and G. Lee, "DDoS attack detection and wavelets," *Telecommunication Systems*, 2005.
[13] Y. Xie and S.-Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 15–25, Feb. 2009.
[14] J. Kaur and Computer Science and Engineering Deptt. PIET, Samalkha, Haryana, India, "Security and ddos mechanisms in internet of things," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 9, pp. 261–265, Sep. 2017.
[15] K. Sonar and H. Upadhyay, "A survey: DDOS attack on Internet of Things," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.
[16] A. D. Keromytis and V. Misra, "SOS: An architecture for mitigating DDoS attacks," *IEEE Journal on selected*, 2004.
[17] Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 12, pp. 1649–1662, Dec. 2007.
[18] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS Attack & its Effect in Cloud Environment," *Procedia Comput. Sci.*, vol. 49, pp. 202–210, Jan. 2015.
[19] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can We Beat DDoS Attacks in Clouds?," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2245–2254, Sep. 2014.

[20] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2017, pp. 1–8.
[21] J. Nazario, "DDoS attack evolution," *Network Security*, vol. 2008, no. 7, pp. 7–10, Jul. 2008.
[22] R. Zhao, S. Wei, and M. Ren, "Combating DDoS attack with dynamic detection of anomalous hosts in software defined network," in *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, Mysore, 2017.
[23] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on DDoS attacks and defense mechanisms," in *Advances in Parallel Distributed Computing: First International Conference on Parallel, Distributed Computing Technologies and Applications, PDCTA 2011, Tirunelveli, India, September 23-25, 2011. Proceedings*, 2011, pp. 570–580.
[24] M. Sachdeva, G. Singh, and K. Kumar, "An emulation based impact analysis of DDoS attacks on web services during flash events," in *2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011)*, 2011, pp. 479–484.
[25] F. Malecki, "Simple ways to dodge the DDoS bullet," *Network Security*, vol. 2012, no. 8, pp. 18–20, Aug. 2012.
[26] G. Somani, M. S. Gaur, D. Sanghi, and M. Conti, "DDoS attacks in cloud computing: Collateral damage to non-targets," *Computer Networks*, vol. 109, pp. 157–171, Nov. 2016.
[27] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Exit from hell? Reducing the impact of amplification DDoS attacks," in *23rd ${USENIX} Security Symposium ({USENIX}$ Security 14)*, 2014, pp. 111–125.
[28] F. Guenane and M. Nogueira, "Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture," *2014 global information*, 2014.
[29] M. Sachdeva, K. Kumar, G. Singh, and K. Singh, "Performance Analysis of Web Service under DDoS Attacks," in *2009 IEEE International Advance Computing Conference*, 2009, pp. 1002–1007.
[30] P. Pandey and Scholar Department of CSE AIST, Sagar (MP), India, "Ddos attack on wireless sensor network: A review," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 9, pp. 227–229, Sep. 2017.
[31] A. Spognardi, M. D. Donno, N. Dragoni, and A. Giaretta, "Analysis of DDoS-Capable IoT Malwares," in *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems*, 2017.
[32] K. Y. Nikolskaya, S. A. Ivanov, V. A. Golodov, and A. S. Sinkov, "Development of a mathematical model of the control beginning of DDoS-attacks and malicious traffic," in *2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS)*, Saint Petersburg, Russia, 2017.
[33] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004.
[34] A. Yaar, A. Perrig, and D. Song, "Pi: a path identification mechanism to defend against DDoS attacks," in *2003 Symposium on Security and Privacy, 2003.*, 2003, pp. 93–107.
[35] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *Proceedings DARPA Information Survivability Conference and Exposition*, 2003, vol. 1, pp. 303–314 vol.1.
[36] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication*, 2004.
[37] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, Apr. 2008.

[38] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Comput. Commun.*, vol. 107, pp. 30–48, Jul. 2017.
[39] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arab. J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, Feb. 2017.