IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Review Paper on Secure Virtualization and Protect Cloud Computing from DoS Attacks

Rahul, Rachith M R, Pavan Kumar VPruthviraj K L
Student
Alvas Institute of Engineering and Technology

Abstract:

Today is the era of cloud computing technology in the IT industry. The most advanced computingarchitecture are being developed and growth in Internet-based cloud computing. By using the collection of networks, integrated, software and hardware-based systems in cloud and distributed computing environment will enhance the flexibility. Beyond the Grid computing and other computing technologies offer several advantages. In this paper we can understand how to achieve secure virtualization using logistic regression and naive bayes algorithms and to protect virtual networks in cloud computing using software-based virtual LAN concepts for implementing in virtualized IT environment. It is important to compare various algorithms for providing security against DoS attack using weka pulg-and-play machine learning solution tool and learn about precision as well as accuracy of those algorithms.

Keywords: Virtual Lan, Grid computing, Logistic regression, Weka, DoS

1. INTRODUCTION

The term "cloud" in cloud computing represents a collection of networks, similar to how a real cloud is formed by water molecules. It provides customer, clients with unlimited access to computing resources as needed. The real meaning of this is emerged through various scientific studies. It is nothing bur the combination of concepts such as service-oriented architecture, meshand distributed computing, and virtualization. A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer network, service, or website by overwhelming it with a flood of illegitimate requests or traffic, rendering it inaccessible to legitimate users. To protect cloud computing from Denial-of-Service (DoS) attacks, employ measures such as utilizing Content Delivery Networks (CDNs) and load balancers for distributed traffic management, designing scalable architectures to handle traffic fluctuations, implementing traffic filtering through firewalls and intrusion detection systems, applying rate-limiting mechanisms to control request volumes, utilizing anomaly detection tools to identify unusual patterns, and leveraging security features provided by the Cloud Service Provider(CSP).

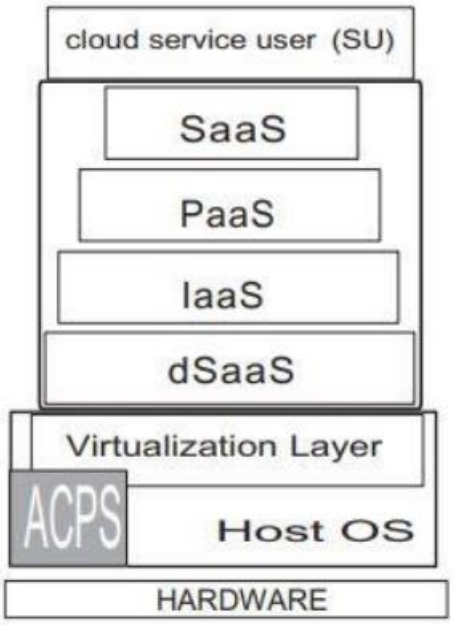

Fig 1. Safety Mechanism for Cloud Computing

The above figure shows safety mechanism for cloud computing. It includes SaaS, PaaS, IaaS, dSaaS. SaaS (Software as a Service) delivers software applications over the internet, allowing users to access and use them without the need for installation or maintenance [14]. PaaS (Platform as a Service) provides a platform with tools and services for developers to build, deploy, can manage applications without accessing with the underlying infrastructure. IaaS (Infrastructure as a Service) offers virtualized computing resources, including storage, networking, and computing power, enabling users to run and manage applications on a flexible and scalable infrastructure. dSaaS (Data as a Service) involves delivering data-related services over the cloud, allowing users to access and utilize data resources without the need for local storage or management. It also shows cloud layers and refined cloud service system [14].

In cloud computing, Virtual Local Area Networks (VLANs) enable the logical segmentation of a physical network into isolated virtual LANs, facilitating enhanced network security, improved performance, and simplified network management by isolating broadcast domains and allowing for efficient traffic organization. In the realm of cloud computing, VLANs provide a means of logically dividing a physical network into distinct, isolated segments, designated by VLAN tags, to enhance security, streamline management, and optimize network performance by isolating broadcast domains and organizing traffic efficiently.

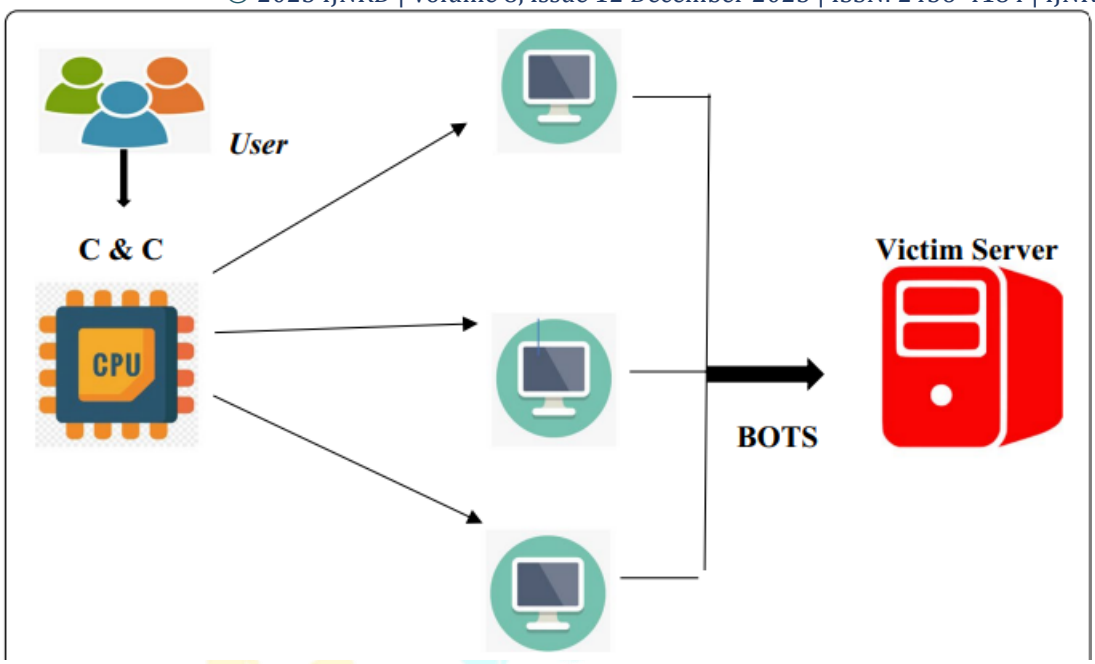

Fig 1.1 DDOS Attack Scenario on Victim Server

A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer network, service, or website by overwhelming it with a flood of illegitimate requests or traffic, rendering it inaccessible to legitimate users. In a Denial-of-Service (DoS) attack, the attacker aims to make a service, network, or website unavailable to its intended users by flooding it with a high volume of requests, consuming its resources, and causing it to become overwhelmed. This will lead to a slowdown or complete unavailability of the targeted system, providing legitimate users from accessing the services provided by the affected entity. DoS attacks can take various forms, such as overwhelming network bandwidth, exhausting server resources, or exploiting vulnerabilities in the target system to disrupt its normal operation [1].

2. Virtualization

Virtualization software is an essential component of cloud computing as it facilitates the creation and administration of virtual machines on physical hardware. With the help of virtualization technologies, multiple operating systems and applications can run on a single physical server, which leads to better resource utilization, flexibility, and scalability.

key aspects of virtualization software in the context of cloud computing:

2.1 Hypervisor (Virtual Machine Monitor - VMM):

The hypervisor, also called as the Virtual Machine Monitor (VMM), is a critical component of virtualization software [3]. It comes in two types: Type 1 Hypervisor (Bare Metal Hypervisor) and Type 2 Hypervisor (Hosted Hypervisor). The former runs directly on the physical hardware to control the hardware compoent and manage guest operating systems, while the latter runs on top of a host OS and is often used for development or testing environments [4].

2.2 Resource Pooling:

Resource pooling is another key aspect of virtualization software that you should know about. It allows the abstraction of physical resources such as CPU, memory, storage, and network into resource pools, which can be dynamically allocated to VMs based on demand, optimizing resource utilization. VMs are isolated from one other, providing security and ensuring that the failure of one VM does not affect others [7]. This isolation is crucial in a multi-tenant cloud environment where more than one users or organizations share the same infrastructure.

2.3 Isolation:

Isolation is a key feature of virtualization that ensures that VMs are distinguish from each other, providing security and preventing the failure of one VM affecting others [6]. This is particularly important in multi-tenant cloud environment where multiple users or organizations share the same infrastructure. By seperate VMs from each other, virtualization provides an additional layer of security and helps to ensure that each user or organization has access only to its resources.

3. Secure virtualization

In the context of cloud computing, secure virtualization software is an essential component that ensures the safety and protection of virtualized environments. With multiple virtual machines (VMs) running on a single physical server, it is crucial to have secure virtualization in place to isolate and safeguard these VMs from potential security threats. By implementing advanced security measures such as secure boot, encryption, access control, and network segmentation, virtualization software can provide a secure and reliable environment for cloud computing. It is imperative to prioritize secure virtualization software to ensure the safety and security of your virtualized infrastructure.

Key aspects of secure virtualization is the use of encryption to safeguard data and communications within the virtualized environment. which helps prevent unauthorized access to sensitive information as it moves between VMs, ensuring data confidentiality. Access controls are another crucial element of secure virtualization [8]. Robust authentication and authorization mechanisms are employed to manage and restrict user access to virtualized resources, make sure that only authorized users or processes can interact with specific VMs. This helps reduce the risk of malicious activities. In multi-tenant cloud environments, secure virtualization acts as a barrier, preventing one tenant from accessing or impacting the resources of another. This isolation is vital for maintaining the privacy and security of each tenant's data and applications. Moreover, secure virtualization contributes to regulatory compliance by implementing security measures that align with industry standards and requirements [9]. This is particularly important for organizations handling sensitive data, as it helps them meet legal and regulatory obligations. By establishing a secure boundary between VMs, secure virtualization mitigates the risk of attacks that target vulnerabilities in shared cloud infrastructures. This not only protects the individual VMs but also enhances the overall security posture of the cloud environment.

Different techniques has been given to identify faults in guest operating systems. For instance, Dan P. et al. proposed a system called "Vigilant" that utilizes virtualization and machine learning techniques to monitor virtual machines through the hypervisor without installing any monitoring agent in the virtual machines [11]. Flavio L. et al. proposed the Advanced Cloud Protection System (ACPS) that monitors and protects the integrity of the OS in guest virtual machines. Periodic monitoring of executable systems is also necessary to conduct of cloud components. Virtual introspection method can be used to deploy guest monitoring machines within the system without being detected by attackers on the guest virtual machine. This way, any suspicious activity on the guest OS can be detected and blocked.

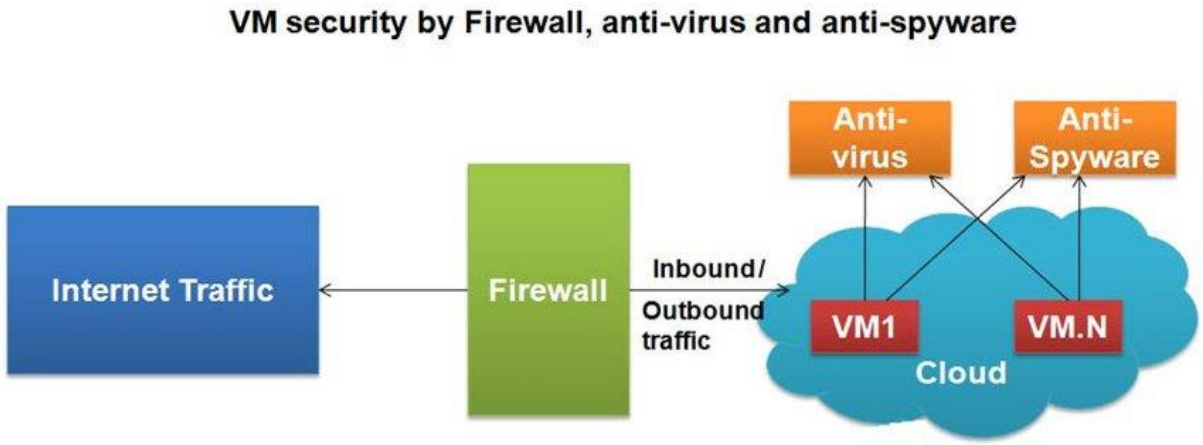

Fig 3.1 Virtual security machine

3.1 Virtual networks

Virtual networks in cloud computing are a fundamental component of modern IT infrastructure, providing a flexible and scalable solution for connecting and managing resources in the cloud. These virtual networks operate on the principles of virtualization, enabling the creation of isolated, software-defined environments that mimic traditional physical networks. Through this abstraction, cloud users can design, configure, and manage complex network topologies without the constraints of physical hardware [2]. Virtual networks in the cloud offer several key advantages, including on-demand scalability, resource optimization, and cost efficiency. Users can define and customize network configurations, such as subnets, security groups, and routing tables, to meet specific application requirements [5]. Additionally, virtual networks facilitate the seamless integration of various cloud services, allowing for the efficient sequence and control of applications across distributed and geographically diverse environments.

4. Virtual LAN:

Regardless of how the underlying physical network is configured, virtual local area networks, sometimes referred to as virtual LANs, are logical groups of computers that has to connected the same local area network (LAN). Network administrators partition the networks into virtual local areas (VLANs). Based on the functional needs of the VLANs, each VLAN is made up of a subset of ports on one or more switches or bridges. This allows computers and devices in a VLAN to interact with each another in the virtual environment as if it were a separate LAN.

It is possible to isolate and logically divide one or more physical LANs into several broadcast domains using a VLAN. Additionally, every broadcast domain is handled differently than other VLANs. Typically, communication is limited to devices that are part of the same VLAN.

By restricting how much traffic an endpoint sees and processes [10], VLANs can enhance device performance. The number of other hosts from which a specific device receives broadcasts is reduced by using VLANs to split broadcast domains. Workstation-generated broadcast traffic will not reach the phones and vice versa, for instance if all desktop voice-over IP phones are connected to one VLAN while all workstations are connected to another. Each has the option to restrict its network resources to only relevant traffic. For every VLAN, engineers can create a different set of traffic-handling rules[14]. They can assist or guarantee the proper functioning of telepresence devices is by establishing rules that provide priority to video traffic on a VLAN that connects conference room equipment.

4.1 RSA Algorithm for Virtual Network:

One important component of cloud data security is the RSA algorithm. It makes use of a public-key cryptosystem, in which encryption and decryption are accomplished using two mathematically related keys: a public key and a private key.

The RSA algorithm functions as follows in cloud computing:

1. Key Generation: A public key and a private key are created by the cloud user.

The user alone has access to the private key, which is kept confidential.

2. Data Encryption: The public key of the cloud service provider is pre-owned by the user to encrypt their data.

This procedure entails using the public key and a mathematical operation known as modular exponentiation to convert the plain text data into an unreadable format.

3. Information Archiving:

Following encryption, the data is transfer to the cloud storage provider.

4. Retrieving and Decrypting Data:

The user use their private key to decrypt encrypted data so they can access it.

The data can only be successfully decrypted and restored to its original plain-text format using the user's private key.

5. DOS attack in Cloud Computing:

A denial-of-service (DDoS) attack involves flooding a target server, service, or network with excessive traffic, making it unusable for legitimate users and overloading it. Think of a huge traffic jam on the digital highway as a mass of data packets instead of cars.

Because cloud computing infrastructure is interconnected, DDoS attacks can be especially harmful. An effective assault can Disrupt vital services: It is possible to make websites, cloud apps, and even entire platforms unusable. Undermine consumer confidence and brand reputation. A company's reputation and client relationships can be seriously harmed by outages and data breaches. Result in monetary losses, Negative effects on sales, efficiency, and client orders can have a big influence on a company [12].

Weka tool:

Weka is a widely used machine learning and data mining software. Developed by the University of Waikato in New Zealand, Weka (Waikato Information Analysis Environment) provides a complete system for data analysis, search and modelling. Friendly interface: Weka provides an intuitive graphical user interface (GUI) that allows users to perform many machine learning tasks without requiring extensive programming knowledge. Differentiator algorithms: It has different machine learning algorithms for tasks such as classification, regression, clustering, common mining rules, and exclusive selection. These algorithms are easy to use for testing and analysis. Pre-processing data: Weka provides pre-processing data, including cleaning, transforming, filtering and rendering of worthless objects. This allows users to efficiently organize data for analysis. Testing and measurement: Allows users to design and run machine learning experiments, evaluate models using a variety of metrics, and visualize results to better understand them. Integration and extensibility: Weka is designed to be easily extensible, allowing users to add new methods, presets, filters, and visualization tools. Compatibility: Supports multiple data formats and interacts with other devices, allowing it to be used in many places and situations. Weka is popular among researchers, students, and machine learning experts due to its accessibility, many layers, and ease of use. It is a great platform to learn machine learning skills and apply them to different data. Plagiarism Remover helps to remove plagiarism from the content whether it is an article, essay, or research paper. The development of this free plagiarism changer is done with modern algorithms that are dedicated to providing accurate results with modern vocabulary. It rewrites data using Natural Language Processing (NLP) and Deep Learning technology which helps to generate plagiarism-free content by keeping the original context of the underlying text. All you need is to copy the content and paste it into the given space to do your content free from plagiarism.

6.1 Weka tool used for DoS attack:

A denial of service (DoS) attack is a cast of cyber warfare that aims to prevent legitimate applications from accessing network infrastructure. Malicious users orchestrate these attacks with the intention of creating a massive influx of traffic in the targeted system's area. This surge in traffic leads to network congestion and drains the resources of the victim system. The attack does not intend to capture vital information or compromise credential files, but instead, aims to render the system inoperable. As a output of the attack, the system may be unable to receive packets, and a three-way handshake, which is necessary to establish a network connection, may fail. It is imperative for organizations to take proactive measures to safeguard against these types of attacks. Organizations can implement measures such as firewalls and load balancers to mitigate the risks of DoS attacks. These measures help to identify and block malicious traffic while ensuring legitimate traffic flows smoothly. By proactively addressing the threat of DoS attacks, businesses can minimize the impact on their operations and protect their reputation. In the procedure of establishing a connection between the client and a server, the server assigns capacity within the connection reservoir and acknowledges the client's request upon receipt. Subsequently, the recipient verifies the connectivity, signaling the successful completion of the process. However, in a scenario where a denial of service (DoS) attack takes place, the perpetrator simulates the connection establishment process, sending photons as expected. Nevertheless, the attacker never receives the provider's final affirmation notification, leaving the relationship incomplete. As a result, the host's system gets exposed to the reservoir space reserved for all unfinished transactions. If the crucial success factors are met, the server's buffer will be full of unresolved attachments, leaving little room for acceptance TCP connections. This effectively renders the server unable to undertake a DoS attack. In their research, Singh KJ et al. illustrate a DDOS assault scenario that manifest how such attacks can be executed [16]. It is important for organizations to implement proactive measures to safeguard against such attacks to protect their systems and networks. Taking preemptive steps like using firewalls, intrusion detection systems, and load balancers can help mitigate the risks of DoS attacks. By providing these measures, organizations can make sure that networks remain secure and operational.

	Total instances	Correctly classified instances	Accuracy	Precision	Recall	Mean Absolute Error	Machine Learning Algorithm used	Class
Training data	14,063	14,063	100	1.000	1.000	0	Logistic Regression	Attack
	14,063	13,929	99.04	1.000	0.981	0.007	Naïve Bayes	Attack
	14,063	14,063	100	1.000	1.000	0	Logistic Regression	Normal
	14,063	13,929	99.04	0.981	1.000	0.007	Naïve Bayes	Normal
Test data	5425	5417	99.85	1.000	0.997	0.0015	Logistic Regression	Attack
	5425	5385	99.26	1.000	0.985	0.0061	Naïve Bayes	Attack
	5425	5417	99.85	0.997	1.000	0.0015	Logistic Regression	Normal
	5425	5385	99.26	0.986	1.000	0.0061	Naïve Bayes	Normal
Validation Data	602	601	99.83	1.000	0.997	0.0017	Logistic Regression	Attack
	602	594	98.67	1.000	0.974	0.0163	Naïve Bayes	Attack
	602	601	99.83	0.997	1.000	0.0017	Logistic Regression	Normal
	602	594	98.67	0.974	1.000	0.0163	Naïve Bayes	Normal

Fig.6.1 Summary of the result of the experimental tool

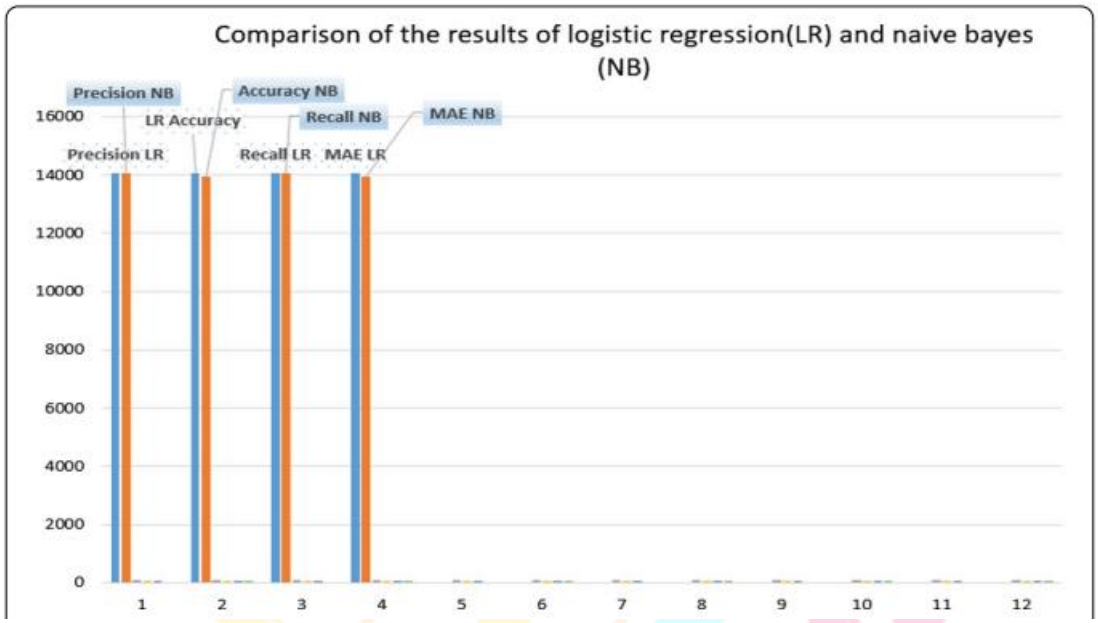

Fig 6.2. Graph comparison of logistic regression and naïve bayes

6.1.1 Algorithm used in DoS attack:

The MLP classification algorithm is highly effective in detecting DDoS attacks with a 98.99% detection rate. It showcases the immense potential of deep learning in cyber threat detection and prevention.

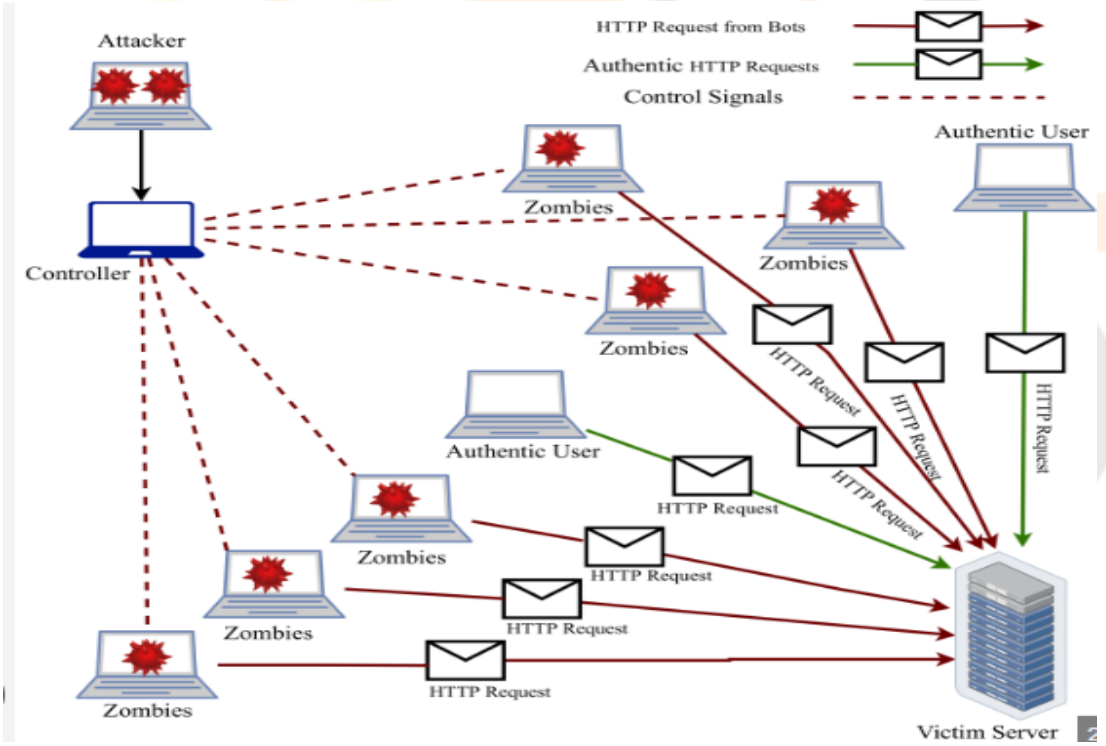

Fig 6.3. DoS Attack mechanism

When writing in Plain English, it's important to consider your target audience and their specific needs. The text should be organized logically, The important data presented first and sentences kept short and to the point. Using familiar language and avoiding acronyms and legal jargon is key. To increase clarity, use active verbs and keep the flow of the text easy to follow. In this case, a Multilayer Perceptron (MLP) has been used as a deep learning

algorithm to make the effectiveness of metrics-based attack detection. The output have been better, with the MLP classification algorithm demonstrating a 98.99% efficiency rate in identifying Distributed Denial of Service (DDoS) attacks. By processing and analyzing network traffic data, the MLP can extract crucial metrics that differentiate normal network behavior from anomalous patterns associated with DDoS attacks. These findings have potential to hold great promise in strengthening cybersecurity measures and mitigating potential threats in network infrastructures.

6. 2 Logistic regression and Nayve bayes:

Logistic Regression is a statistical method used for binary classification tasks, predicting the chance of an observation belonging to a particular class. Despite its name, it's a classification algorithm, not a regression algorithm. This model employs a logistic function to model the understanding between the independent variables and the binary outcome, fitting a sigmoid curve that maps input features to a chance between 0 and 1. This algorithm is particular suited for scenarios where the dependent variable is categorical and dichotomous, such as predicting whether an email is spam or not, or if a patient is likely to have a certain disease based on medical test results. Its simplicity and interpretability make it a widely used tool, especially when there's a need to understand the impact of individual predictors on the probability of a specific outcome [12]. This algorithm is particular suited for scenarios where the dependent variable is categorical and dichotomous, such as predicting whether an email is spam or not, or if a patient is likely to have a certain disease based on medical test results. Its simplicity and interpretability make it a widely used tool, especially when there is a need to analyze the impact of individual predictors on the probability of a specific outcome.

Naive Bayes is a probabilistic classifier based on Bayes' theorem with an assumption of independence between features. Despite its simplicity and 'naive' assumption of feature independence, it often performs remarkably well in various classification tasks, especially in text classification and spam filtering. This algorithm calculates the probability of a data point belonging to a certain class given its feature values by considering the joint probability of all the features being observed in that class [15]. Despite the 'naive' assumption, Naive Bayes can be surprisingly effective in many real-world scenarios. It's fast, works well with high-dimensional data, and requires minimal training data. However, Naive Bayes can struggle when faced with correlated features, as it assumes complete independence between them. Additionally, it might not capture complex relationships or interactions among features, which could limit its performance in certain situations.

Acknowledgments. The authors extend their heartfelt gratitude to Alvas Institute of Engineering and Technology, India, for generously providing the essential resources and support that made the research and development of the Secure Virtualization and protect cloud computing from DoS attack and user experience possible.

REFERENCES

[1] Luigi Coppolino; Cloud security: Emerging threats and current solutions (2016).
[2] Ananthanarayanan R, Gupta K et al Cloud analytics: do we really need to reinvent the storage stack? In: Proc of Hot Cloud (2009).

[3] Armbrust M et al Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report

(2009).

[4] Priscila Cedillo, Emilio Insfran ,Jean Vanderdonckt , Empirical Evaluation of a Method for Monitoring Cloud Services Based on Models at Runtime

[5] Bodik P et al Statistical machine learning makes automatic control practical for Internet data centers. In: Proc Hot Cloud (2009).

[6] Mrs. Ashwini Sheth, Sachin Shankar Bhosale; Research Paper On Cloud Computing (2021)

[7] Chandra A et al Nebulas: using distributed voluntary resources to build clouds. In: Proc of Hot Cloud (2009).

[8] Chang F, Dean J et al Bigtable: a distributed storage system for structured data. In: Proc of OSDI (2006).

[9] Mine Omurgonulsen , Pretty Singla, Merve Ibis Cloud Computing: A Systematic Literature Review and Future Agenda(2021).

[10] Church K et al, on delivering embarrassingly distributed cloud services. In: Proc of Hot Nets (2008).

[11] Selecting cloud computing software for a virtual online laboratory supporting the Operating Systems (2022).

[12] Cloud Computing on Wikipedia, en.wikipedia.org/wiki/ Cloud computing, 20 Dec 2009

[13] Sajid Habib Gill Mirza Abdur Razzaq, Muneer Ahmad, Fahad M. Almansour; Security and Privacy Aspects of Cloud Computing (2022)

[14] Pankaj Saraswat, Anjali; International Journal of Innovative Research in Engineering & Management(IJIREM)ISSN:23500557,Volume9,Issue1,February202,https://doi.org/10.55524/ijirem.2022.9.1.103 Article ID IRP229201 (2022)

[15] Journal of Network and Computer Applications Volume 34, Issue 4, July 2011, Pages 1113-1122

[16] Kimmi Kumari, M. Mrunalini: Detecting Denial of Service attacks using machine learning algorithms (2022)