DETECTION OF DOS ATTACKS USING ANOMALY BASED IDS

[1] M.Prabu, [2] N.Prabhakaran
[1]Assistant Professor, [2]Assistant Professor,
[1] Department of ECE
[1] Misrimal Navajee Munoth Jain Engineering College, Chennai -97, India.

Abstract: The internet is accessed by a large number of people worldwide within their respective domains. When clients and servers exchange messages, their activity can be observed in log files. These files provide a detailed description of network activity, including IP addresses, login and logout durations, and user behaviour. Various types of internet attacks occur. This paper focuses on Denial of Service (DoS) attacks, which can be identified through pattern recognition techniques in data mining. DoS attacks are particularly dangerous because they overload an organization's IT resources with imitation messages or multiple requests from unauthorized users, putting those resources at risk.

Index Terms - Attacks, DoS, Data mining.

I. INTRODUCTION

In order to address possible detections and mitigations of attacks on Cloud Computing, it is first necessary to examine the types of attacks and attackers that pose a threat to this technology. There are various forms of attacks that can occur within the Cloud infrastructure and its environment, including Distributed Denial of Service (DDoS) attacks. In a DDoS attack, a collection of remotely-controlled bots, also known as "zombies", is coordinated by a master entity to overwhelm the target system. Attackers can be classified into three categories based on their location, motivation, and level of activity in the attack. Cloud computing infrastructures can be compromised in various ways, whether the attack originates from within or outside the system. The scope of an attack can varies greatly depending on the perpetrator. System administrators take appropriate measures to exclude the attacker and ensure a quick recovery, followed by subsequent investigations. DDoS attacks are particularly disruptive, as they involve a large number of hosts, often without the owner's knowledge. The ultimate goal of a DoS or DDoS attack is to compromise the availability of the Cloud, targeting the victim's communication bandwidth, computational resources, memory buffers, network protocols, or application processing logic. These attacks can occur remotely or locally from the victim's or user's service.

The internet plays a significant role in facilitating services such as banking, electronic commerce, social networking, and newsgroups. However, Denial of Service (DoS) attacks can disrupt these services, hindering their growth and continuity. DoS attacks prevent legitimate users from accessing specific internet services by overwhelming the network services or victim resources. These attacks consume the victim's resources, making it impossible to respond to authenticated user requests. To prevent such attacks, network architecture should be designed to identify intruders who target the system. Despite being one of the oldest internet threats, DoS attacks remain a serious problem and pose a high risk to networks worldwide. Detecting DoS events can be challenging, as these attacks are constantly evolving. They can cause complete unavailability of services, which can result in significant financial losses for businesses. Misuse-based detection systems can detect attacks by monitoring network activities and matching them with existing attack signatures. However, these systems are easily evaded by new or modified attacks. The primary objective of this project is to identify Denial-of-Service attacks using data mining techniques. Such attacks are dangerous and put IT resources at risk by keeping the server busy with imitation messages and repeated queries. The proposed goal is to develop a Denial-of-service attack detection system.

Cloud computing is a cutting-edge technology that aims to provide end-users with instant access to resources. By leveraging the distributed resources available on the internet, cloud computing enables customers to perform computations without the need to install software on their own computers. Customers only pay for the resources they consume, while the cloud service provider takes care of all the computational requirements, shielding the user from any underlying complexities. According to NIST, cloud computing has five key characteristics: on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service. Cloud services are available in three basic forms: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The evolution of cloud computing is towards providing everything as a service (XaaS). However, as more data migrates to the cloud, attackers are increasingly targeting vulnerabilities associated with cloud computing to steal sensitive data.

System analysis is a problem-solving technique that involves breaking down a system into its individual components in order to study how effectively they work and interact with each other to achieve their intended purpose. This process involves collecting and interpreting relevant information to diagnose issues and ultimately recommend improvements to the system. The current network-based detection systems are divided into two main categories: misuse-based detection systems and anomaly-based detection systems. Misuse-based detection systems detect attacks by monitoring network activities and identifying matches with the existing attack signatures. However, even with high detection rates to known attacks and low false positive rates, they can be easily evaded by new attacks or variations of existing attacks. In contrast, the proposed system uses anomaly-based detection to recognize attacks. This method effectively detects known and unknown DoS attacks by learning the patterns of legitimate network traffic only, without requiring any attack relevant knowledge. To enhance and speed up the process of MCA, a triangle-area-based technique is proposed. In product development, it is essential to distinguish between the baseline functionality necessary for any system to compete in the product domain and features that differentiate the system from competitors' products. Such strategies have significant implications for software architecture, as the architecture must not only support the Software requirements specifications of the initial release but also the Software requirements specifications of the initial products.

II. Related Works

Outlier detection technique was proposed in the development of an intrusion detection system to mitigate Denial of Service (DoS) attacks [1]. Characteristics of the Web accessing DoS attacks were analyzed and proposed an active defense model [2]. Various outlier detection approaches were discussed from the perspective of data mining [3]. Firstly, a novel multi-chunk, multi-level ensemble technique for stream data classification was proposed, which improves upon existing single-chunk single-level ensemble techniques. Secondly, the effectiveness of this technique was proven through theoretical analysis. Finally, the proposed ensemble technique was applied to detect P2P botnet traffic, resulting in better detection accuracies compared to other stream data classification techniques [4]. Survey of various types of HTTP-based Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks was conducted to identify the most effective specifications for a protective framework against HTTP-based DoS and DDoS attacks [5]. Entropy based System and Anomaly detection System are merged to providing multilevel Distributed Denial of Service (DDoS) [6]. Signature based intrusion detection system and anomaly-based intrusion detection system were combined to form Hybrid IDS [7].

III. Technology Used

The .NET Framework is a modern computing platform that simplifies the development of applications in the highly distributed environment of the Internet. At the core of the .NET Framework is the common language runtime, which manages code at execution time and provides services such as memory and thread management, as well as remoting for more security and robustness. The runtime operates on the principle of code management, whereby code that targets the runtime is known as managed code, while code that doesn't is referred to as unmanaged code. The .NET Framework is a comprehensive, object-oriented set of reusable types that can be used to develop a range of applications from traditional command-line or GUI-based apps to modern ASP.NET applications like Web Forms and XML Web services. Additionally, the .NET Framework can be hosted by unmanaged components, allowing software environments to leverage both managed and unmanaged features. The .NET Framework also supports the development of third-party runtime hosts, offering flexibility and extensibility.

The common language runtime of the .NET Framework provides robust security features that allow Internet-deployed software to have rich features. Code access security is enforced by the runtime, which grants managed components varying degrees of trust based on factors such as their origin and the types of operations they can perform. Additionally, the common type system (CTS) enforces code robustness by verifying types and codes, ensuring that all managed code is self-describing. The managed environment provided by the runtime helps to eliminate common software issues.

The common language runtime not only enhances security and code robustness, but also boosts developer productivity and application performance. Developers can write applications in their preferred programming language and still use the runtime, class library, and components written by other developers in different languages. The runtime's design optimizes performance as well, as managed code is compiled just-in-time (JIT) to run in the native machine language of the system it runs on. This feature enables the runtime to be hosted by high-performance server-side applications such as Microsoft SQL Server and Internet Information Services (IIS).

IV. System Implementation

System design involves defining the system's architecture, components, modules, interfaces, and data to meet specific requirements. This process applies systems theory to product development and intersects with disciplines such as systems analysis, system architecture, and systems engineering. Prior to planning a new business system or replacing an existing system, it is important to thoroughly understand the old system and identify how it can be improved. Unified Modeling Language (UML) is a graphical visualization language that utilizes symbols and connectors to create process diagrams. It is commonly used to model computer programs and workflows, and can also be applied to visualize website structure and user interfaces. System architecture is shown in Figure 1.

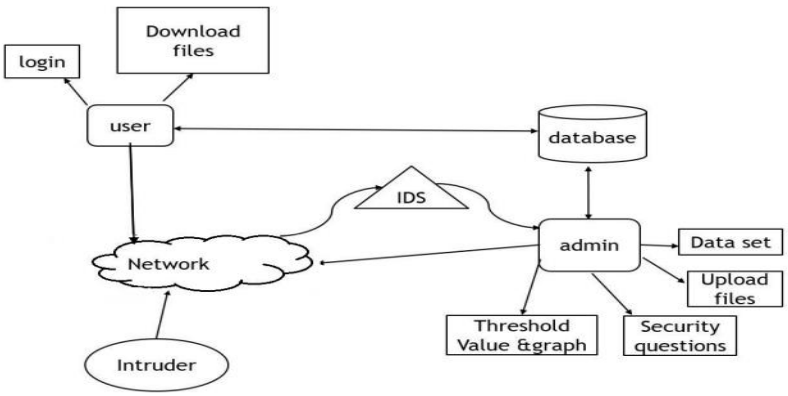

Figure. 1 System Architecture

Login Module: Logging in enables a user to access a restricted page that is not visible to unauthorized individuals. Once the user is authenticated, their login token can be used to monitor their activity on the site. This is achieved through the user registration module, which requires all new users to register. Each user is assigned a unique password to accompany their username. To access their account, users must provide their valid login credentials, which ensures authentication and security for their account.

File Uploads/Downloads Module: The file uploads module is primarily intended for uploading data to the cloud. However, it can also be used to detect any misconduct that occurs during data transfers from one authorized user to another. This module provides a detailed view of the uploaded file, allowing users to easily access and review file information.

Threshold DoS Attacks: Threshold refers to a specified value that is associated with a polled data statistic. When data is collected for this statistic, it is compared with the threshold value. If the collected data does not meet the threshold value, it may indicate that the performance of the device or network could be compromised. The threshold value can be set with a specific level, such as the maximum, minimum, or equal value.

Graph Details: The graph displays the number of Denial-of-Service (DoS) attackers detected in a network over a certain period, with details of the month and time shown. A chart or graph is a visual representation of data, where information is conveyed through symbols like bars, lines, or pie slices. Charts can represent numerical data, functions, or qualitative structures and provide valuable insights.

V. Conclusion and Future Scope

In this paper, data mining techniques were applied to identify Denial-of-Service (DoS) attacks, which pose a significant threat to IT resources. These attacks overload servers by generating imitation messages and repeated queries, leading to congestion and decreased performance. The paper discusses cyber security, cyber-crime types, clustering, outliers, and pattern recognition. The pattern recognition data mining technique was applied to the log file, and a threshold value was set. If the number of similar requests received at the server is greater than the threshold value, it is considered an attack, and the administrator is notified. This approach effectively identifies DoS attacks as they involve multiple identical requests to mitigate server performance. To combat Distributed Denial-of-Service (DDoS) attacks, a comprehensive real-time defense framework close to the attack source with participation from various service providers offering source address validation and filtering features would be the best approach. Such a defense mechanism could be developed in the near future.

References

[1] Ibrahim Salim, M. and Razak, T. A. 2016. A study on IDS for preventing Denial of Service attack using outliers techniques. IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India. 768-775.

[2] Jianpeng Zhao, Shize Guo, Kangfeng Zheng, Xinxin Niu and Yao Jiang. 2010. An active defence model for Web Accessing DoS attacks. IEEE International Conference on Information Theory and Information Security, Beijing, China. 314-318.

[3] Khan, M., Pradhan, S.K., Khaleel, M.A. 2014. Outlier Detection for Business Intelligence using data mining techniques. International journal of Computer Applications. 106(2): 0975 -8887.

[4] Masud, M.M and Gao,J.Khan. 2008. Peer to Peer Botnet Detection for Cyber Security: A Data Mining Approach. In proceedings: Cyber-security and information Intelligence research workshop. Oakridge national Laboratory, Oakridge.

[5] Saleh, M.A and Abdul Manaf, A. 2014. Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks. International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, Malaysia. 63-267.

[6] Syed Navaz, A.S., Sangeetha, V and Prabhadev, C. 2013. Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud. International Journal of Computer Applications, 62(15): 42-47.

[7] Vanitha, D and Chandrasekar, R. 2013. Detection of flooding DDOS attack using anomaly and signature-based intrusion detection system. International Journal of Engineering Research and Technology (IJERT), ICSEM-2013 Conference Proceedings.