A SURVEY ON SEQUENCE NUMBER ENCODING TO MITIGATE DOS/DDOS ATTACKS IN CLOUD ENVIRONMENT

Bhoomi Ramanandi[1], Prof. Manoj Patel[2]
L.D.College of Engineering (I.T.), Gujarat, India

Abstract: A literature survey on In the present world of information technology, Cloud computing is considered the best option for information storage permanently in the third party cloud servers and cached temporarily on clients. This technology represents both, an efficient technology to provide computing infrastructure as well as computer resources and services. As this system is so complex and distributed, it becomes a very easy target for intruders by various types of attacks including Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attack which utilize the entire resources like CPU, Memory, etc and makes the server to starve. The main aim of this scan is to hinder intruders to hit or bend to one will the data by Transmission Control Protocol (TCP) Mitigation Strategy which uses the SYN Cookie to prohibit the clash in the cloud to avert the attack in which the server ignores the connection packets when it does not receive the correct Acknowledgement (ACK) from the client which requested the connection The server here uses many layers of security out of which one is to encode the sequence number where the algorithm XTEA is modified for providing more security in less computation time and to prevent various attacks.

Keywords: DoS/DDoS, Virtualization, SYN Cookie, Hop-Count Filtering, Sequence number, Message Authentication Code

I. INTRODUCTION

Cloud computing system includes various service oriented paradigms, multi-tenancies, on demand elasticity etc. All of these are very vulnerable to cyber-attacks and can pose a threat to data of single individual as well as the entire system. Also as cloud has various clients, all of them with different service as well as security requirements. The main issue is the data leakage between the user and the server. There have been many approaches developed for this, but the direct attacks on virtual machines cannot be prevented after an extent. The modified XTea algorithm used in this approach will prevent the disclosure of the sequence number which is followed by various other steps for security enhancement and to prevent denial of service and distributed denial of service attacks. Along with the lure to use the cloud computing system as it provides efficient use of computing services and infrastructure there also poses a threat for users to worry about their data and also security at the time of data transfer. To provide an efficient and secure system there needs to be approaches developed to overcome the attacks on the virtual machines as well as to prevent data leakage.

II. LITERATUREREVIEW

This section represents the work done by other research people related to detection and prevention of Dos/Ddos attacks in cloud environment using various methodologies.

R. Aishwarya [1] proposed a technique In the given paper, two layers of security is being supplied in order to provide protection against DoS and DDos attacks. Namely:Control Packet Security and Data Packet Security.Various algorithms are used at both the layers and the legitimate client from the spoofed ones providing security for the data packets allowing the clients to use the resources of the cloud server more effectively. This proposed method is very efficient in all the ways to prevent the attacks by encoding the SYN packet and providing security to data and its implementation is also adaptable. The only drawback is that a more reliable and robust algorithm can be provided for encoding the sequence number. Niladree de [2] proposed a technique, the Modified XTEA architecture is well suited for devices in which low cost and low power consumption are desired. The proposed folded architecture achieves good performance and occupies less area than XTEA. This compact design was developed by thorough examination of each of the components of the Modified XTEA algorithm. The encryption speed, functionality, and cost make this solution perfectly applicable for resource constrained applications in cloud and other networks. In this paper, the 232 bit modulo addition at the time of encryption and the 232 bit modulo subtraction at the time of decryption are replaced by N-mix and I-N-min functions respectively.In this modified algorithm for encoding there are many attacks such as chosen plain text attack,12-round impossible differential characteristic ofXTEA and 8-Round Related Key Truncated DifferentialCharacteristic attacks can be prevented. This algorithm can be implemented in combination with other algorithms to prevent dos/ddos attacks. Cheng Jin Haining Wang Kang G. Shin [3], proposed a paper in which, a hop-count-based filtering scheme is depicted that detects and then removes spoofed IP packets to save system resources. Based on the analysis using actual network measurements, author showed that HCF can remove about 90% of spoofed traffic. Moreover, even if an attacker is aware of HCF, he cannot easily circumvent HCF. In this paper a hop-count-based filtering schemethat detects and then removes spoofed IP packets to save systemresources. Based on the analysis using actual networkmeasurements, we showed that HCF can remove about 90%of spoofed traffic. Moreover, even if an attacker is awareof HCF, he cannot easily circumvent HCF. Our experimentalevaluation demonstrates that HCF can be efficiently implementedinside the Linux keRnel. In this paper a systematic approach for setting parameters of HCF is required also it needs to be developed for window system along with Linux kernel. Raneel Kumar, Sunil PranitLal, Alok Sharma[4] proposed the main focus of this paper was on how to detect DoS and DDoS attacks. It is depicted in such a way that it does not compromise the privacy of the cloud user or one who has access to cloud.HP Helion Eucalyptus Cloud is used to create an IaaS cloud for the experimentation and created cloud platform consisting of various virtual machines.The proposed method can efficiently stand against the denial of service attacks. This research can focus on measuring the target VM's performance under various DoS attacks thus determining the impact of each DoS attack on the target VM. In addition, the performance of the proposed DoS IDS under normal and DoS attack scenarios can be evaluated. This will show the system resource (CPU, memory) overhead produced by the DoS IDS when it is in execution in the cloud environment. OsvariArsalan [5] in her paper, the scheduling algorithm XTEA is modified by changing the static key into a dynamic one to avoid several attacks that are being done on the XTEA algorithm.Here, the key for the odd and even rounds are changed and there are two different formulas which calculate a sub master key differently for each and every round.. Biometrics such as fingerprint, eye retina, iris, face, voice and gait offer a more reliable means of authentication. However, due to huge biometric data and multipart biometric measures, it is challenging to design and develop an accurate as well as a fast biometric matching system. Fast fingerprint indexing is one of the most inspiring issues encountered in fingerprint identification system. In this paper, they presented a specific contribution by introducing a novel robust indexing. From security point of view this method is better than the original XTEA, it takes same time to execute as that of XTEA, but it requires 24 bits more memory to store the extra dynamic keys generated every time.

III. CONCLUSION

By studying various papers and approach using various algorithms such as hop count filtering and modified XTEA for encryption of sequence number, and also the filtering of packets that reach the server providing yet more security.. By using the modified XTEA the time complexity can be reduced as use of modulo addition is replaced with bitwise operations. Due to two level of security it is more secure and effectively resisting DoS and DDoS attacks. Also the time is reduced for computing the SYN packet which provides more efficiency and security.

REFERENCES

[1] Intrusion detection system- An efficient way to thwart against Dos/Ddos attacks in the cloud environment, R. Aishwayra

[2] A Modified XTEA, Niladree De, JaydebBhaumil.

[3] Hop-Count Filtering: An Effective Defense Against Spoofed Traffic, Cheng Jin Haining Wang Kang G. Shin

[4] Detecting Denial of Service Attacks in the Cloud, Raneel Kumar, Sunil PranitLal, Alok Sharma

[5] Modification of key scheduling for security improvement in XTEA, OsvariArsalan

[6] Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants, Creighton T. R. Hager, Scott F. Midkiff, Jung-Min Park, Thomas L. Martin

[7] TEA, David Wheeler, Roger Needham, Cambridge university.