Attack Behavior Approach in Slow HTTP DoS Detection

Tran Cong Manh* and Nguyen Huu Hung

***Abstract*—Slow HTTP Denial of Service attack (DoS) is unpretentious but impressive effect in knocking down the opponent. The principle of the attack is quite simple however its detection is complicated. A criminal can open lots of connections to the server by initiating HTTP requests and keep them opening. There are many detections analysis and studies, however at slow DoS attack is still threatening and dangerous. In this paper, TCP/IP packet analyzed, and behavior based to detect Slow HTTP DoS attack is proposed.**

***Index Terms*—Denial of service, slow DoS, HTTP, cybercriminal**

I. Introduction

Application layer attacks pose an ever-serious threat to network security for years since it always comes after a technically legitimate connection has been established. In recent years, cyber criminals turn to fully exploit web as a medium of communication environment to lurk a variety of forbid-den or illicit activities. Web applications are becoming more and more popular and web-based systems are an indispensable foundation for other types of applications such as desktop or mobile applications. As a result, this is fertile ground for cybercriminals using the Hypertext Transfer Protocol (HTTP) protocol to attack systems. Normally, classic DoS makes a server become down or hung by depleting the network/server resource through sending huge requests or packages to that server as shown in Fig. 1.

Slow HTTP DoS is rising as an impressive effect attack in knocking down the opponent. The principle of Slow DoS attack is quite simple by creating many connections to the server but not closing them. Criminals do not need to launch attacks massively but slowly and are difficult to detect. Slow DoS attacks description and taxonomy of slow DoS attacks to web applications can be found in [1].

In this paper, TCP/IP packet analyzed, and behavior based to detect a Slow HTTP DoS attack is proposed. The strength of the solution is that it is simple, easy to deploy and has high reliability, which can be performed on both client and server side under attack.

II. Related Works

There have been many studies on the Slow HTTP DoS attack type shown in the research publications [2]- [10]. An analysis on how to create an effective Slow Read attack is provide in [2]. Accordingly, the Slow Read DoS Attack by a single attacker can be prevented by adequate security settings of Web server and applying countermeasure such as Mod-Security. However, these countermeasures are not effective against distributed Slow Read DoS Attack (Slow Read DDoS Attack).

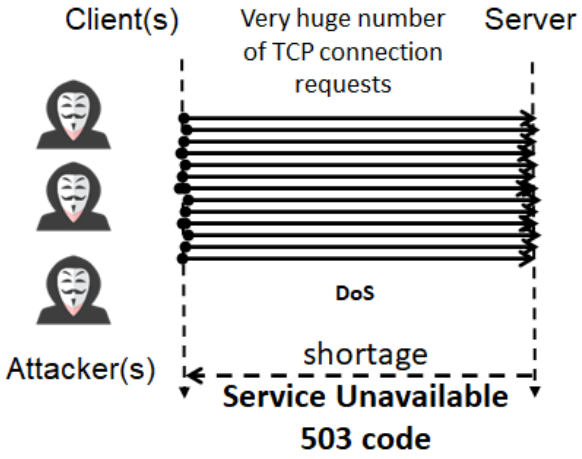

Fig. 1. A sample of classic DoS attack.

An architecture Slow HTTP attacks, allowing to implement the developed algorithm is proposed in [3]. The process of attack detection in [3] is implemented based on a Markov model the behavior of the web server, the model parameters are the statistical characteristics of incoming, outgoing traffic, as well as the dynamics of resource use web server. However, the result of this method is not clearly.

A defence method against large-scale distributed Slow HTTP DoS attack is proposed in [4] by disconnecting the attack connections selectively by focusing on the number of connections for each IP address and the duration time. However, the experimental just effectively against from 30 attackers with thresholds setting properly [4]. Distributed DoS attack is not limiting the attackers at the same time.

III. About Slow Http Dos Attack

HTTP stands for Hypertext Transfer Protocol; HTTP is used in www (world wide web) for the purpose of creating a connection platform between client and server. Normally a web access sends a request to the server and receives a response from that. Request/Response will be done as soon as possible. A sample of a HTTP flow and structure as show in Fig. 2.

A sample of classic DoS attack is shown in Fig. 1, but Slow DoS attack has a different approach with two types of attacks: Slow Read and Slow Post (Slow Send).

The Slow Read attack exploits the GET method of HTTP and sends a request to get a large amount of data to the server but slowly reads the response data from the server. Server cannot push client accept all data as soon as possible. This

Manuscript received January 23, 2023; revised March 23, 2023; accepted May 5, 2023.

Tran Cong Manh and Nguyen Huu Hung are with the Le Quy Don Technical University, Hanoi, Vietnam.

*Correspondence: manhtc@gmail.com (T.C.M.)

will force the server has to open the connection and wait until the attacker has finished reading the data it responds to. The client needs to maintain reading data to ensure that the response from the server is not timeout. The longer the attacker reads, the more processing resources the server must spend and leads to server crashes. A methodology of Slow Read attack type is shown in Fig. 3, and a simulation of data exchange between client and server in this type of attack is described in Fig. 4.

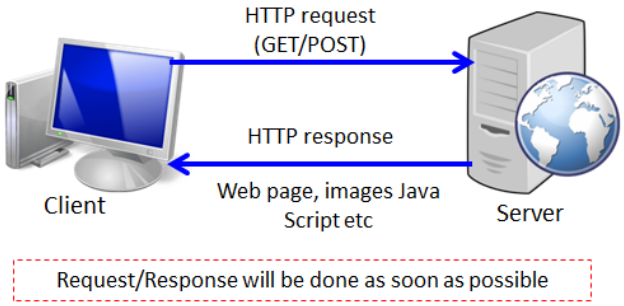

Fig. 2. A sample of classic DoS attack.

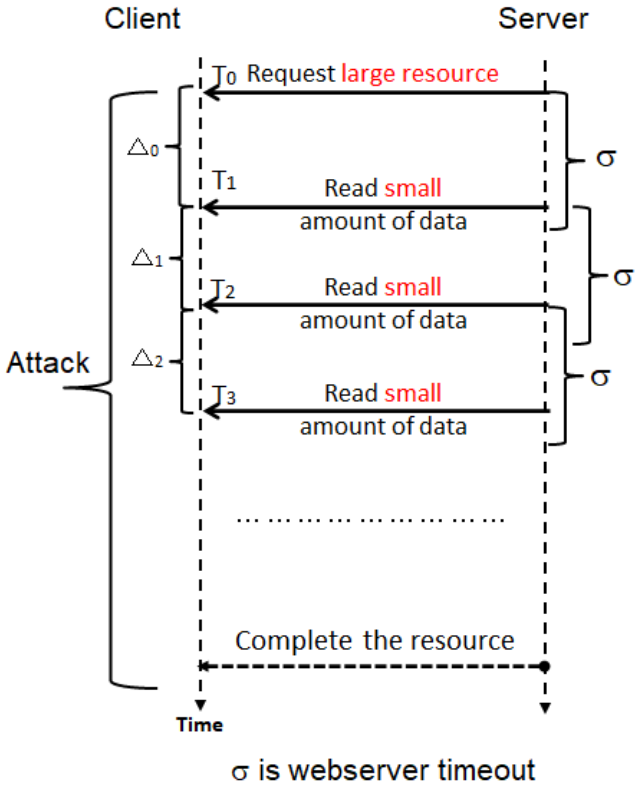

Fig. 3. Slow Read attack methodology.

The Slow Post attack has an approach that uses the POST protocol, but instead of slowly reading the response data from the server, it will delay the request to the server. The principle of slow sending is also implemented to ensure that the sending command is not timeout causing the server to open the socket and maintain resources to receive requests from the client. The slower the client sends, the more resources the server must maintain, leading to the server crashing

A methodology of Slow Post attack type is shown in Fig. 5, and a simulation of data exchange between client and server in this type of attack is described in Fig. 6.

IV. Monitoring and Analysis

To observe and analyze Slow DoS attack method, a tool, as show in Fig. 7, is written in C# language and tested on Windows operating systems using IIS 7.0 and Apache 2.4.7 web server which is run on Ubuntu. The goal of this tool is to evaluate the parameters for the attack to take place successfully.

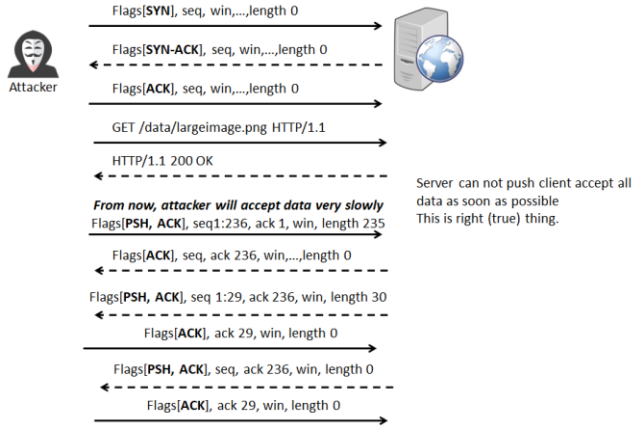

Fig. 4. A simulation of data exchange between client and server in slow Read attack.

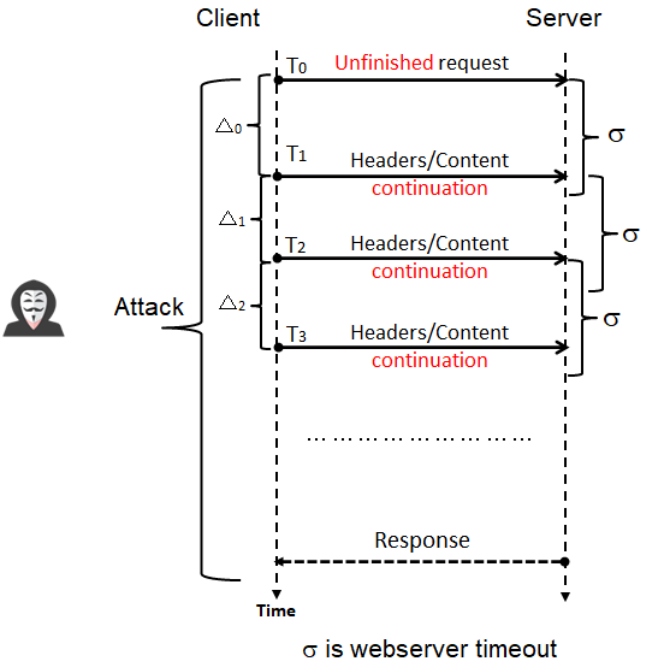

Fig. 5. Slow post attack methodology.

After making many observations and experiments with different numbers of connections, representatives of which are shown in Fig. 8-Fig. 10, the results show that with IIS 7 minimum 10 concurrent requests are required to cause the server to hang and 1010 concurrent requests are required to cause the server to return a 503 error; And also in Apache 2.4.7, the server does not return an error but may cause the server to hang with 200 concurrent connections. Besides, a very special thing, the amount of data that needs to be exchanged between the client and the server does not need to be too large. Exchange data needs to be just over 30 bytes and maintain a slow read/response time of 30s. In experiment, at normal condition of user usage, there is no behavior like this.

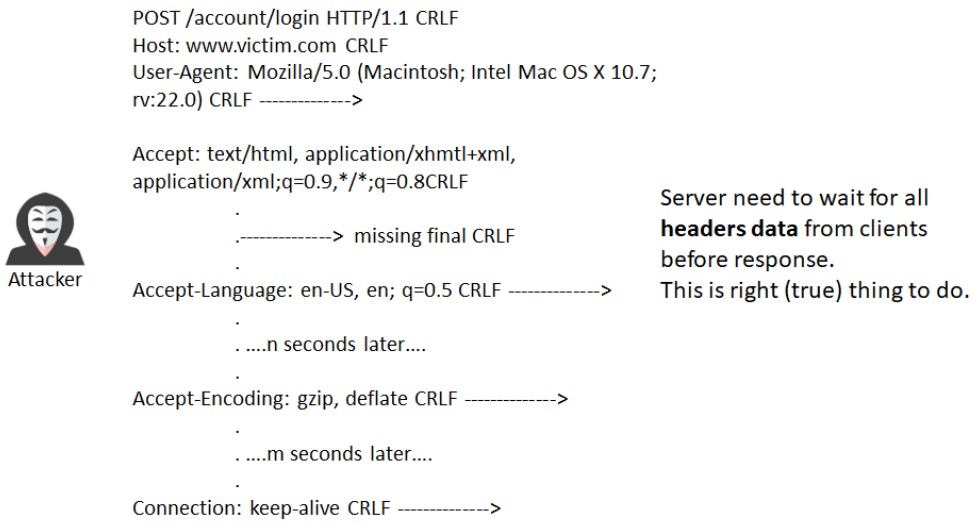

Fig. 6. Slow Post attack data exchange to server process

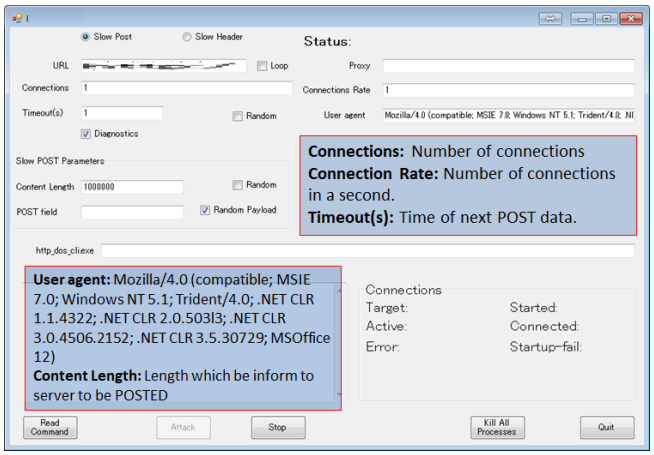

Fig. 7. Experimental tool for monitoring and analysing.

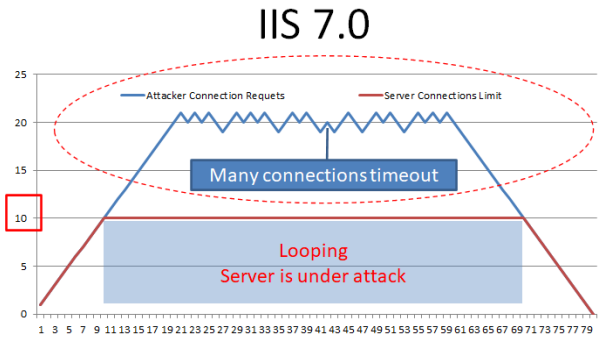

Fig. 8. Experimental attack on IIS 7.0, with 40 concurrent requests at rate: 1 request per second

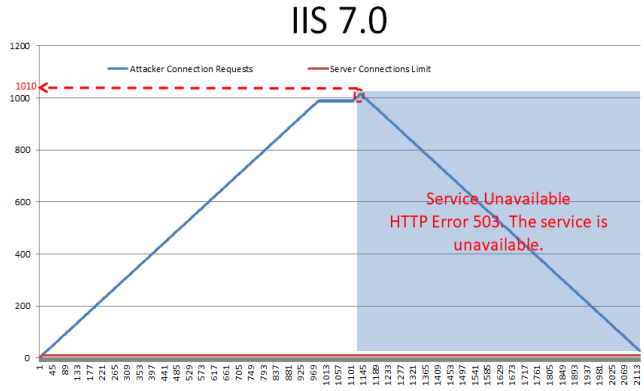

Fig. 9. Experimental attack on IIS 7.0, with 1100 concurrent requests at rate: 1 request per second.

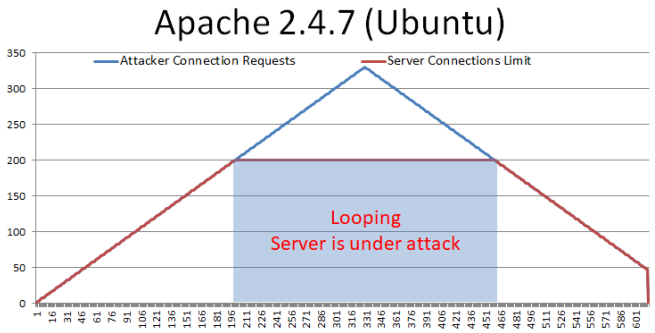

Fig. 10. Experimental attack on Ubuntu with Apache 2.4.7, with 500 concurrent requests at rate: 1 request per second.

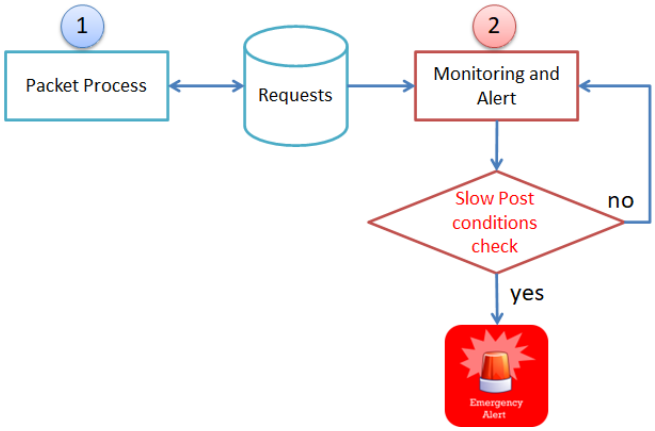

Fig. 11. Detection proposal at client side.

V. Detection Method Experimental

Based on the observations and analysis in section 4, a Slow HTTP attack detection method is proposed with the description shown in Fig. 11.

As shown in Fig. 11, there are two main processing phases: packet processing (1) and monitoring and alerting (2). In which, the packet processing step will perform the decomposition of the packet's parameters, put in a queue for processing (a database of requests), the purpose of this step is to record the connections being opened and the data is in slow processing (reading slowly or sending data to the server) by the attacker. The details of the algorithm are shown in Fig. 12.

The second phase is an important next step, which will be based on the parameters of the number of parallel connections, as well as the delay time between the 2 packets sending from which the alert is raised. The details of the parameters and the processing diagram are shown in Fig. 13.

For experimental, Slow DoS attack tests need not be complicated from multiple distributed sources. The parameters of the number of concurrent connections and the frequency have been set in the 11 to 1010 solution with IIS and Apache, the proposed solution can detect attacks. However, with a small number of connections less than 11 it can't be detected, although the attack is still there. If an attacker performs a distributed attack, other approaches are needed.

VI. Conclusion

In this paper, a new approach has been proposed and experimented in detecting Slow DoS attack. Slow DoS attack behavior has been carefully observed and analyzed through a few parameters of TCP/IP packets.

The experiments were implemented in real environment with two popular types of web servers, IIS and Apache. The results show that the solution is capable of detecting Slow DoS attacks well. However, the solution needs to be improved to adapt to the distributed attack pattern with each attack point having a low number of connections (less than 11) to the server.

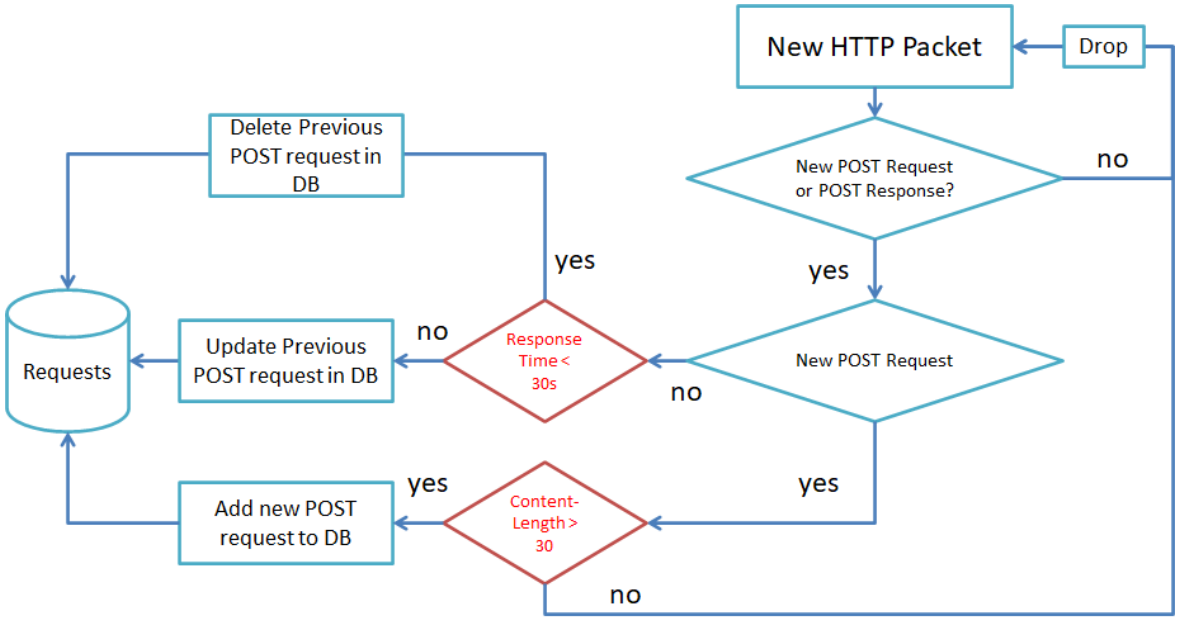

Fig. 12. Packet process phase.

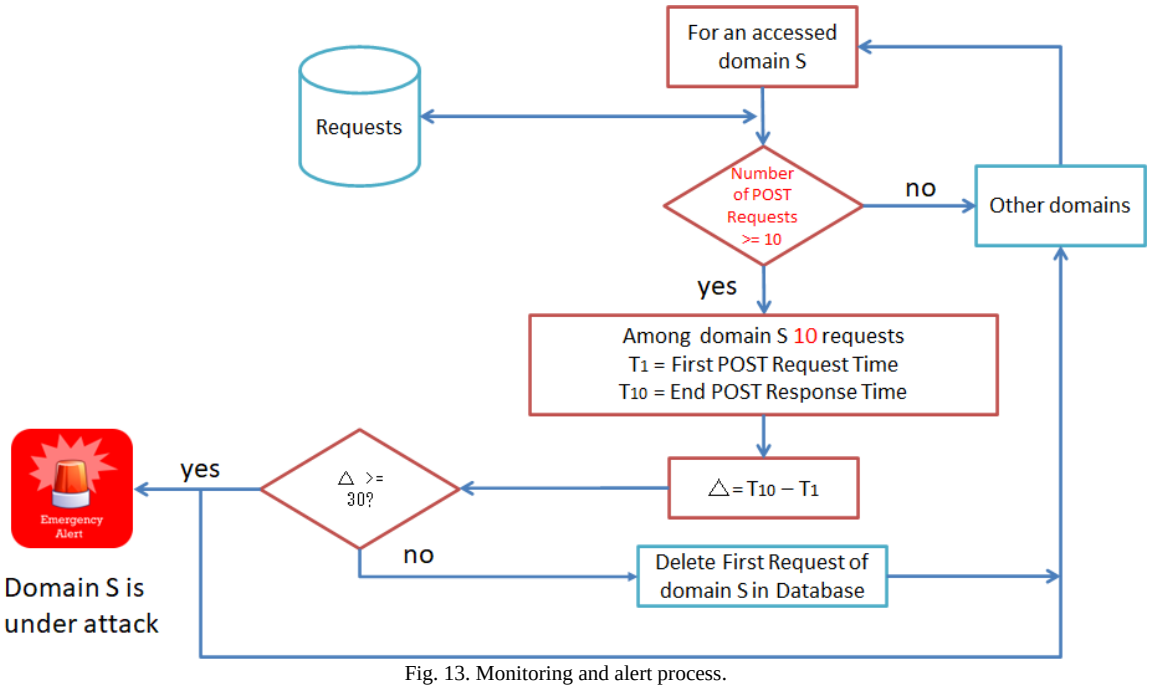

Fig. 13. Monitoring and alert process.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Tran Cong Manh (1st author) is the main author participated and conducted in all research stages with ideation, research implementation steps. He wrote chapters 1, 2, 5, 6 of the paper, in that chapter 5 is shared with Nguyen Huu Hung.

Nguyen Huu Hung (2nd author) is a participating author helps to collect data and join the experimental process. He wrote chapters 3,4, 5 (shared with Tran Cong Manh) of the paper.

Both authors also do cross review the paper.

References

[1] E. Cambiaso, G. Papaleo, and M. Aiello, "Taxonomy of slow DoS attacks to web applications," *Communications in Computer and Information Science*, vol 335, 2012.

[2] J. Park, K. Iwai, H. Tanaka, and T. Kurokawa, "Analysis of slow read DoS attack," in *Proc. 2014 International Symposium on Information Theory and its Applications*, 2014, pp. 60-64.

[3] I. Duravkin, A. Loktionova, and A. Carlsson, "Method of slow-attack detection," in *Proc. 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, 2014, pp. 171-172.

[4] T. Hirakawa, K. Ogura, B. B. Bista, and T. Takata, "A defense method against distributed slow HTTP DoS attack," in *Proc. 2016 19th International Conference on Network-Based Information Systems (NBiS)*, 2016, pp. 152-158.

[5] O. Yevsieieva and S. M. Helalat, "Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment," in *Proc. 2017 4th International Scientific-Practical Conference Problems of Info communications*, 2017, pp. 519-523.

[6] C. Calvert, C. Kemp, T. M. Khoshgoftaar, and M. M. Najafabadi, "Detecting slow http post dos attacks using netflow features," in *Proc. the 32nd International FLAIRS Conference*, 2019, pp. 1–4.

[7] N. Muraleedharan and B. Janet, "A deep learning based HTTP slow DoS classification approach using flow data," *ICT Express*, vol. 7, no. 2, 2021, pp. 210-214.

[8] E. Cambiaso, M. Aiello, M. Mongelli, and I. Vaccari, "Detection and classification of slow DoS attacks targeting network servers," in *Proc. 15th International Conference on Availability, Reliability and Security* USA, pp. 1–7, 2020.

[9] C. Kemp, C. Calvert, and T. M. Khoshgoftaar, "Detection methods of slow read DoS using full packet capture data," in *Proc. 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*, 2020, pp. 9-16.

[10] M. Sikora, R. Fujdiak, K. Kuchar, E. Holasova, and J. Misurec, "Generator of slow denial-of-service cyber-attacks," *Sensors*, vol. 21, no. 16, 2021.