Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 5, May 2020, pg.60 – 65

SDN BASED PACKET INJECTION ATTACK PREVENTION IN CLOUD ENVIRONMENTS

S.E.Viswapriya[1]; K.Saipranay[2]; B.Yaswanth[3]
Assistant Professor, Student, Student
Department of Computer Science, SCSVMV University, Kanchipuram, India

Abstract– Software-Defined Network (SDNs) architecture can easily be attacked by a malicious user in order to prevent an acceptable level of service. This SDN architecture is a novel network architecture which contains both control plane and data plane has been decoupled with each other. It is not similar to traditional networking architecture because it acts as the centralized controller so that it provides a global view as well as the environment applications can be programmable interfaced with the architecture. Many researches addressed about various kinds of threats such as spoofing, tampering, information disclosure, denial of service, flow table overloading and so on. The main goal of novel SDN design is to solve three security threats such as flow table overloading, spoofing attack, and isolating anomaly packets from normal packets. The increased reach of cloud computing is achieved in the field of computing devices. The major challenge in cloud environment is to secure the reliable data from unauthorized users. Therefore, the most hot research topic is to secure the SDN components by improving the SDN architecture. In this paper, we propose SDN based early pollution detection algorithm able to spot the presence of an attack while fetching the data from cloud storage during the normal disk reading operations. Also to detect the polluted content hashing methods are used. A web based intrusion detection and prevention system using policies. User data confidentiality and integrity has been gained by protecting user data privacy.

I. INTRODUCTION

In order to build an easy programmable and flexible network this Software-Defined Network (SDN) architecture will separate hardware and software components. By reducing the complexity of switches in the network the dynamic and adaptive network management was enabled by the Software defined network. The entire network has been controlled and monitored by the SDN controller plane and the organization of data plane components is based on the SDN controller instructions.

The information gathered by the controller from the network components that includes switch information, location of hosts and link status, and has the complete knowledge about the global network topology. The developers can customize the controller tasks by adding their innovations, policies and applications on top of the controller is also allowed by SDN architecture.

There is no specific mechanism to detect illegal access while exchanging data between the two networking devices. Moreover, the SDN switch cannot prevent the packet injection attack without installing temporary instructions from the controller because the SDN switch has no way of making local decisions.

In the cloud environment, packet injection attack is very common. One of the major concerns for all stakeholders in cloud environment is to secure the outsourced data. A set of malicious entities named as pollution attacks will attempt to corrupt the stored data in cloud. This is one of the major risks that affects

the cloud data security. The major key concerns for users, system designers, and service providers is the act of securing the outsourced data. Pollution attack plays the major role in threats of data integrity among various risks to data security. So the SDN architecture will leads to ensure the ability data trustworthiness. In this attack, the control of one or more storage resources was taken by malicious entities to corrupt or pollute data. The major scope in cloud environment is to develop an automated prevention measures in order to detect early pollution attack.

II. LITERATURE SURVEY

According to Levente Butty´an, L´aszl ´o Czap, Istv´an Vajda, Pollution Attack Defence for Coding Based

Sensor Storage, in this approach, the new decoding algorithm has been developed in order to make possible to find adverbial blocks using one or more encoded block than decoding algorithm. This particular scheme is well suited for sensor networks requirements. The source and storage nodes which has very low computational and communication overhead has been operated. But the need of additional computations has been performed by the collector node. It will not work in environment such as sharing keys, secure channels PKI are available. This is because this approach never used the cryptographic techniques.

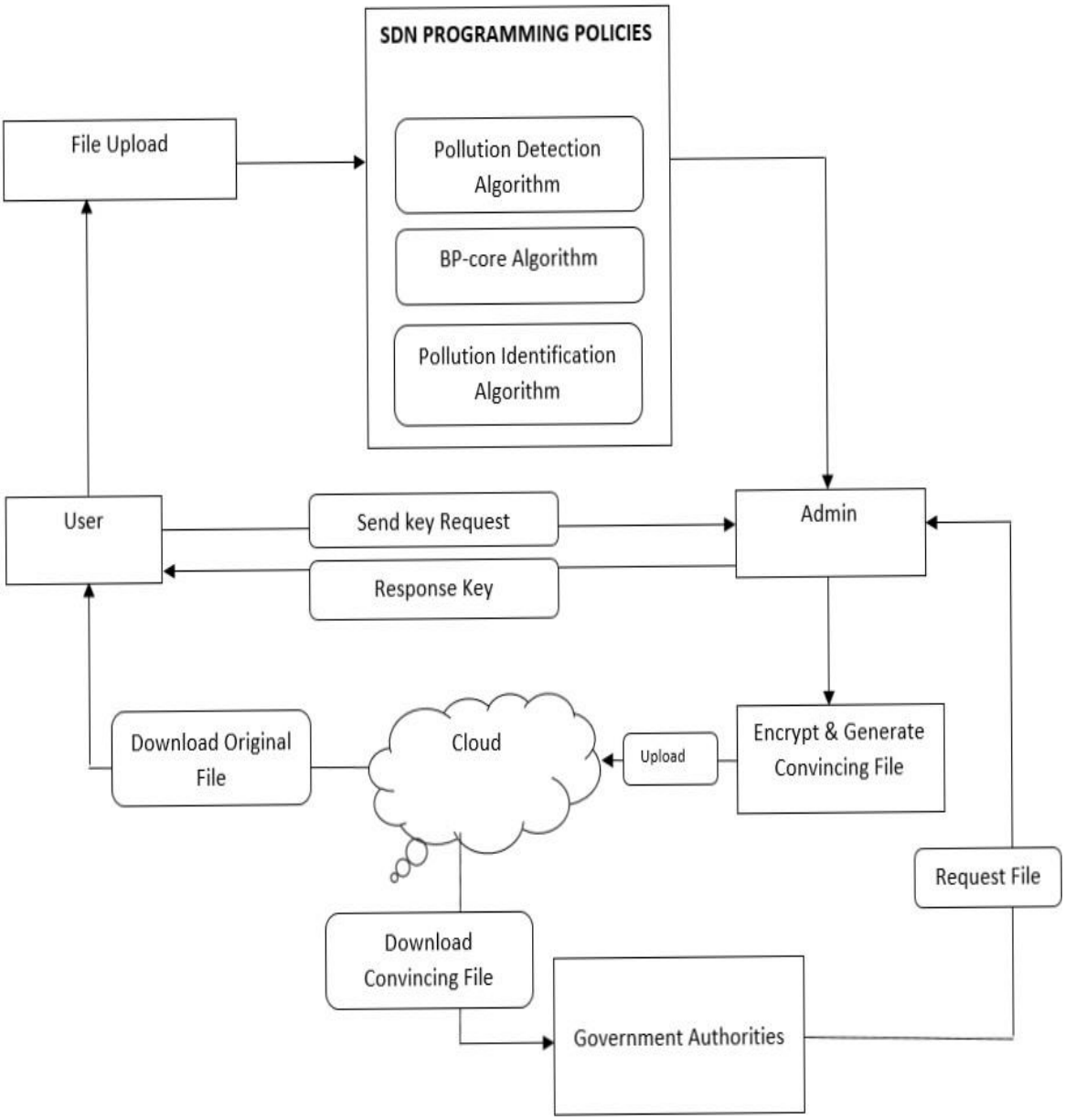
According to author HassanKooshkaki ; BehzadAkbari ; Abdollah Ghaffari Sheshjavani, A Multi-Level reputation-based pollution attacks detection and prevention in P2P streaming, the more important networks such as peer to peer networks which performs high scalability, low cost point of view. These kind of networks are more popular platform for video streaming. Some attacks like pollution attack are made serious challenge due to peer to peer networks. The malicious users will produce the fake content and that content will replace the original content and that same will be broadcast to the various networks. Due to this we will be getting only poor quality of service and the user will also be dissatisfied. Even the controller process cannot able to control these diffusions, and very soon the polluted content can sent to different networks. So in this approach the multilevel mechanism has been developed based on CDN – P2P networks. This mechanism is used to calculate the reputation and also it use temporarily blocked policy.

According to Parihar Vimladevi Mishrilal, Rohini Dattatrey Patil, even though the cloud computing is more popular, it lacks in supporting for computer forensic investigations. The major role of computer forensic is to inspect various logs such as process logs, networks logs. Along with data packets, a polluted packets were injected. In this approach, the storage frameworks has been designed with coding based square level distributed format. The sending packets must be verified at one stage. The verified has been allowed for further procedures. But the unverified packets will not be allowed for further procedures. They should be detected and discarded because they are considerable malicious packets. With the help of this technique the pollution has been removed before it reaches to the destination. Therefore the pollution attacks can be removed so the throughput and performance of transmitted data has been increased.

III. ACTUAL WORK

ARCHITECTURAL DIAGRAM:

In mechanism of detecting the corrupted packets, it allows the normal packets to mix with corrupted packets, and then it detects the corrupted packets. But it is vulnerable to security threat and widely used. The attackers easily inject the corrupted packets in the network. Allowing the entire set of packets it may have chance of getting infected the server too. In real time environment the most common attack is HTTP parameter pollution attack. In order to reveal the user secrets and confidential data on cloud.

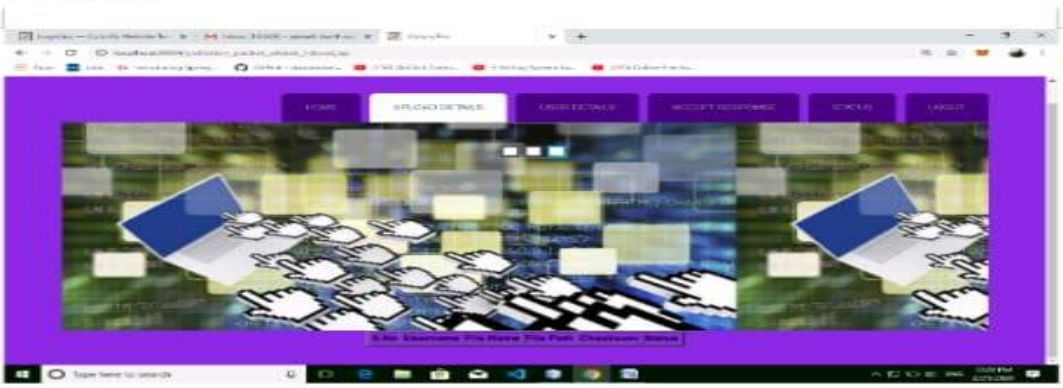


The various modules for this approach are given as follows. They are User Registration & Validation, SDN BASED SOFTWARE COMPONENTS TO PREVENT PACKET INJECTION ATTACK, Transforming data into fragments, Pollution attack detection, Hashing Method, Convincing file creation, RC5 encryption, Cloud Storage

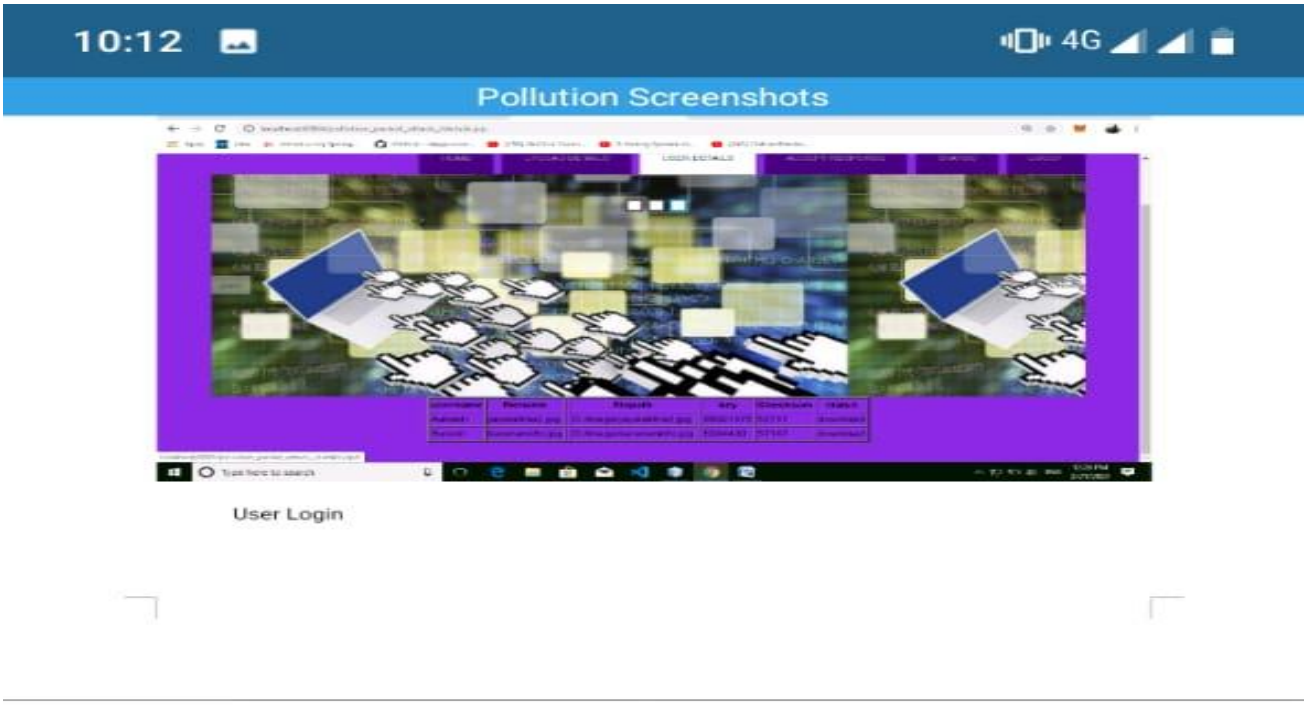
Upload details

Admin Panel

Upload details

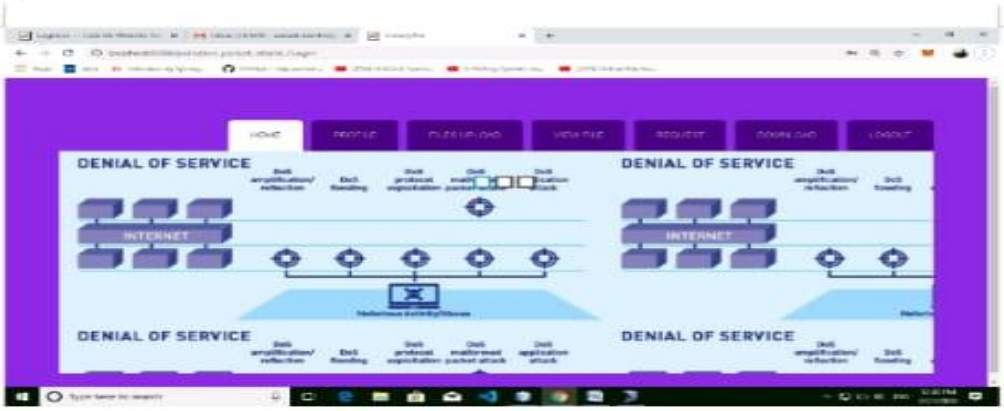


User Details



User Login

Upload details



Profile

File Upload

IV. CONCLUSION

In this paper, In order to check the data integrity during normal read operations, Pollution detection mechanism in a cloud based storage system. Also the malicious (dangerous) nodes are identified in the proposed system. During transmission the hash values are integrated and comparison made with the result and the received hash value from the content distribution network (CDN) servers to determine whether the transmitted data is polluted or not provides high security.

REFERENCES

[1]. D. B. Rawat et al, "Software defined networking architecture, security and energy efficiency: A survey," IEEE Communications Surveys and Tutorials, vol. 19, no. 1, pp. 325–346, 2017.

[2]. S. Deng et al, "Packet Injection Attack and Its Defense in Software-Defined Networks," IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 695–705, 2018.

[3]. T. A. Pascoal et al, I. E. Fonseca, and V. Nigam, "Slow TCAM Exhaustion DDoS Attack," in 32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC). Rome, Italy: IFIP, May 29–31 2017, pp. 17–31.

[4]. Q. Yan et al, "Software-Defined Networking (SDN)and Distributed Denial of Service (DDoS)Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," IEEE Communications Surveys and Tutorials, vol. 18, no. 1, pp. 602– 622, 2016.

[5]. Openflow switch specification, version 1.3.5 (protocol version 0x04),Open Networking Foundation, Tech. Rep. ONF TS-023, 2017.

[6]. K. Bhushan et al, "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)based Cloud Computing Environment," Journal of Ambient Intelligence and Humanized Computing, pp. 1–13, 2018.

[7]. M. Dhawan et al, "SPHINX: Detecting Security Attacks in Software-Defined Networks." in NDSS, vol. 15, 2015, pp. 8–11.

[8]. S. Shin et al, "Attacking Software-Defined Networks: A First Feasibility Study," in Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. Hong Kong, China: ACM, August 16 2013, pp. 165–166.

[9]. M. Antikainen, et al, "Spook in Your Network: Attacking an SDN with a Compromised OpenFlSwitch," in 19th Nordic Conference on Secure IT Systems (NORDSEC), Tromsø, Norway, October 15–17 2014, pp. 229–244.

[10]. H. Wang et al, "OF-GUARD: A DoS Attack Prevention Extension in Software-Defined Networks," in Fourth Annual Open Networking Summit 2014, Santa Clara, CA, USA, March 3–5 2014.

.

