DDoS Attacks Simulation in Cloud Computing Environment

Shakti Arora, Surjeet Dalal

Abstract: Cloud Computing Is Increasing Its Reach To The Edge Of The Computing Devices. Day By Day Dependency Of The Users Is Increasing On Cloud. Infrastructure As A Service Model Is The Widely Adopted And Used Model Of Cloud Computing Where Storage Is The Primary Concern To Be Shared And Used. Security Of The Shared Storage Is The Major Challenge, A Number Of Techniques And Security Algorithms Are Designed To Provide The Security And Accuracy Of The Data. We Designed A One Strong Integrity Security Algorithm That Provides The Integrity Verification Of The Stored Data Without The Intervening The Role Of Tpa. The Data Stored On The Server Can Be Compromised With Number Of Security Attacks; We Studied The Major Security Attacks That Are Affecting The Data. In This Paper We Will Demonstrate The Attack Simulation Of Ddos Attack And Calculated The Effects Of Attacks On Running System And Performance Of The System Under Critical Timings Of Attack. The Result Of The Attack Simulation Shows That The Designed System Is Stable And Working Efficiently After The Attack. The Trust Level Achieved Is Approximately Similar To The Original Trust Achieved Without Injecting The Attack.

Keywords: attack, Virtualization,Poly1305, Integrity, hybrid

I. INTRODUCTION

Security deals with accuracy, safety and privacy of the data. Amazon, IBM, Microsoft are nowadays providing the infrastructure support to the users which helps in managing and running any small enterprises to large commercials. There is always a research going on in the backend to cover the security holes and make the system more attack proof and secure. Beyond that users are trying to setup with their own clouds and generating revenues. A number of cloud computing vulnerabilities that arises in cloud computing security

A threat is a potential cause of an incident that may harm to an enterprises/organization system, and weaknesses in the system called vulnerability, activated by threat. Data Breaches occurs when private or personal data related to an entity is accessed by some unauthorized or unwanted entity. In 2017 A million of records stored on cloud server were lost and breached by hackers. Approximately 143 million people were affected Equifake breach. In May 2017 cloud server provided one login access and identity management was hacked.

Revised Manuscript Received on November 05, 2019.

Now days small or medium sized companies are shifting their services to the cloud to get better business opportunities and infrastructure at negligible cost. Cloud computing is a style of computing where Information technology based services are delivered as a service to end users or external customers using internet.

Cloud computing is having a great business opportunity in the market nowadays. cloud providers ensure that , they will get security for all the services and applications running and consumed by cloud. If anything goes wrong CSP will be responsible for all loss and security issues. Cloud offers benefits like low cost, disaster recovery, pay-per basis, fast deployment, protection against attacks, on line low cost storage solution, pay per basis usage of licensed software. Cloud proposed a tremendous advantages , which makes the life of developers and entrepreneur more easier and flexible. But according to the survey, many of the major companies are challenging the security aspects of cloud, 74% of IT professionals and CIO's referred security as a top challenge and preventing the adoption of cloud service models. According to analysis of current market, usage of cloud application is predicted approximately $95 billion and 14% of the software market will be completely shifted to cloud. Cloud computing moves the application software and business software to large data centers, data management and services should be trust worthy. Cloud security challenges include, accessibility, integrity, virtualization, SQL injection, vulnerability, cross site scripting. Following are the major issues that directly affect the cloud communication.

1) Threat to data
2) API vulnerabilities
3) Insider attacks
4) Shared resources and technology
5) Low and weak cryptography

II. RELATED WORK

Naseer[11] discussed the cloud computing principles, cloud computing security requirements, security threats, security attacks and mitigation techniques and future research challenges of cloud security . Akhilesh[12] discussed the handling of DDoS attacks in distributed cloud computing environment, also proposed the defense mechanism adopted for DDoS attacks .in this paper a relationship between SDN and DDoS identified. Vidhya[13] discussed the possible types of DDoS attacks and their defense mechanism in different types of attacks with their affects and results.

Subhashini[]did a survey of the possible security risk that pose a threat to the cloud security issues related to the service delivery model of cloud communication are focused. Sujata[9] proposed a CAPTCHA based security technique called two tier CAPTCHA which increases the resistance against attacks by applying more queries and combinations. It makes the system hard to reach and approach for any attack and increases the security level. Desh Mukh[] proposed four different techniques to handle the DDoS attack in cloud computing and most importantly focused and gave a solution to cloud mitigation techniques to handle the attacks and secure the system.

III. OUR CONTRIBUTION

The main goal of the attacker is to get access of the main data stored on the cloud and preventing the resources to reach to the client; both of the conditions are harmful to the system. On the hosting platform there is not much that can be done against attacks according to the customer perspective, traffic of large DDoS attack can affects the cost of services on the cloud, so there is a great need to explore the CSP market and precautions taken by CSP against the different attacks

Testing of attack in proposed system

We have designed a hybrid integrity verification algorithm that is working in the combination of SSS and AES Poly (1305). AES Poly 1305 is defined in standard integrity library and working on the hardness of the key shares generated by the Shamir secret sharing algorithm. The proposed algorithm is designed for decentralized cloud computing environment which also removes all the problems mentioned in the centralized cloud computing.

The proposed system is implemented in the cloud environment with the help of open stack cloud computing software. Open stack is Open source cloud computing software which is used to create public and private cloud. A cloud node can be set up and with the dashboard provided in the interface of the open stack , private or public existence of the nodes can be designed in the cloud.

In this research article, the proposed designed cloud node is tested under attacks simulation and performance analysis is done in the basis of the performance.

IV. DDOS ATTACK

Distributed denial of service attack is the mostly configured and injected attack in the cloud communication where huge traffic is generated by malicious nodes to the targeted nodes which make the system slow or unresponsive. It overload the system with unnecessary traffic, these types of attacks are very dangerous for the users and create flooding. All the computational power is consumed to handle the flood. In Oct 2018 attack on DNS company called dyn get down many websites Finally cloud systems get slow down and all legitimate users lose access and availability to the cloud users. If hackers are using zombie machines then DDos attacks becomes more dangerous.

There are different types of DDoS attacks

- Bandwidth based attack
- Volume based attack
- Application layer attack/layer 7 attack
- UDP flood attack
- ICMP flood attack
- Ping of death
- Smurf attack

4.1 ATTACK SIMULATION

Main issue in the cloud computing is to handle the inside and outside attacks that can harm the complete system and especially the data placed on the cloud. Data on cloud is increasing day by day, so the chances of attacks are also increasing; we have implemented two attacks to check the performance of the system under traffic measurement. UDP Flood attack and IGMP flood attack.

4.2 ABOUT TOOLS

Net stress- is a network stress testing and used for introducing DDoS attacks. This tool can be used to check the performance throughput of the network. This tool is used to set the benchmark of the network performance, for example, we want to check the performance of the system and want to set the benchmark under some conditions then net stress can be used. It works in wired as well as Wi-Fi networks .it's working in layer three i.e network layers and generated traffic for TCP as well As UDP connections

Wireshark- is network protocol analyzer which checks the traffic running on network at microscopic level and filter out the unauthorized or unwanted traffic that harm the network system. Wireshark can run on any platform like windows, Linux, FreeBSD, NetBSD etc. it is the widely adapted tool in the industry in today's scenario.

4.3 UDP FLOOD ATTACK

A UDP flood does not exploit any vulnerability. Sending a large number of datagrams from spoofed IP to target server and due to heavy traffic server is unable to process every request..

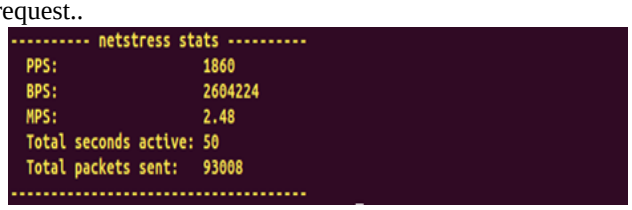

Figure 1: Summary of Traffic File Generated By UDP Attack

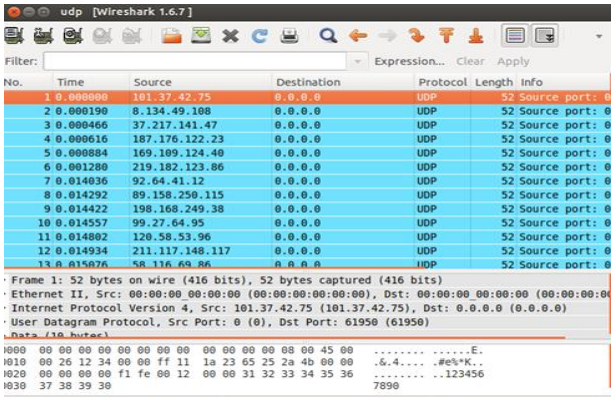

Figure 2: Analysis of Traffic File with UDP Attack Using Wireshark

4.4 IGMP FLOOD ATTACK

IGMP (Internet Group Management Protocol) is a connectionless protocol like UDP. IGMP is a protocol used to manage multicast members in TCP/IP.

Like UDP flood, IGMP flood does not exploit any vulnerability. Just sending any type of IGMP packets continuously makes server overwhelmed from trying to process every request.

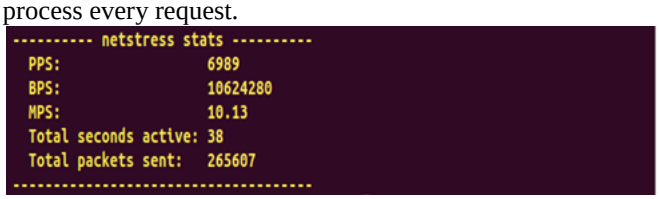

Figure 3: Summary of Traffic File Generated by IGMP Attack

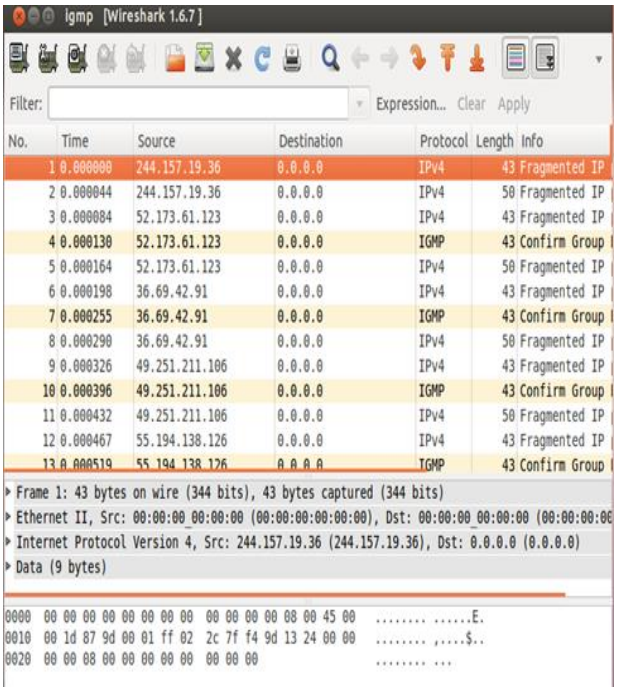

Figure 4: Analysis of Traffic File with IGMP Attack Using Wireshark

V. RESULT ANALYSIS

After injecting the flood attacks, approximately for 50 seconds and 38 second where traffic generated in these duration is approximately 93000 and 265000. Trust metrics are calculated instantly after applying the attacks and rust factor is calculated and analyzed.

Table 1 Attack simulation results

Attack	Time	Traffic
UDP flood attack	50 seconds	93008
IGMP flood attack	38 second	265607

VI. CONCLUSION

After injecting the UDP and IGMP flood attacks and monitoring the traffic for different intervals of time, trust values are calculated for the running system and find out that there is no such variation or degradation integrity, reliability and turnaround time of the cloud set up node

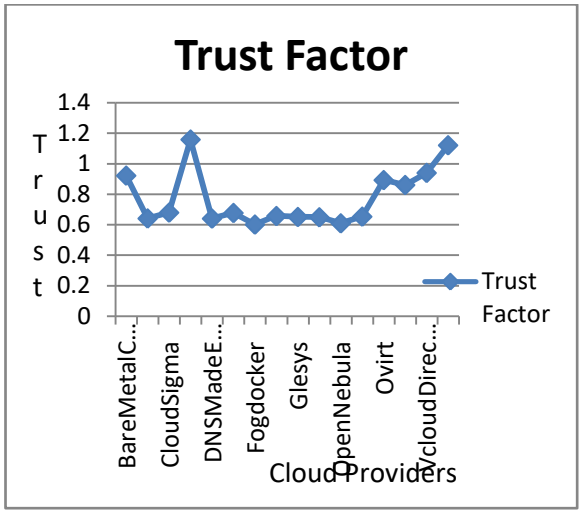

Figure 5:- Trust evaluation after attack

REFERENCES

1. Salman iqbal,liana mat kian, bubak dhaghighi, muzammil hussain, suleman khan, Muhammad khurra khan, kim kwang, Raymond choo, " On cloud security attacks: A taxanomy and intrusion detection and prevention as a service, " *in journal of network and computer applications* , volume -74, PP. No 98-120, 2016.
2. Priyanka Chauhan, Rajender Singh, " Security attacks on cloud computing with possible solutions,", in *international journal of advanced research in computer science and software engineering*," vol-6, issue 1, PP.No 92-96, 2016.
3. Ardian J Duncan, Sadie Creese, Michal Goldsmith, " Insider attacks in cloud computing," in IEEE 11th national conference on *Trust security and privacy in computing and communication*, 2012.
4. Meiko Jensen, joy chwenk, nibs gruksha, lugi lo lacano, " on technical security issues in cloud computing in "IEEE international conference on cloud computing,",PP. No. 2009
5. Ajey singh,, manesh Shrivastav, " Overview of attacks on cloud computing," in international *journal of engineering and innovative technology*, vol-1, issue-4 , 2012.
6. Rashmi V. Deshmukh, Kailas K. Devadkar, Understanding DDoS Attack & Its Effect In Cloud Environment, in *Procedia Computer Science*, volume -49, PP.No. 202 – 210, 2015.
7. A.M lonea, D.E. Popescu,H. Tianfiekd," Detecting DDos attacks in cloud computing environment*," in International journal compute communication*, Vol-8, issue-, PP.No 70-78, 2013,
8. Victoria, NSW,"EDOS-shield- A two step mitigation technique against DDos attacks in cloud computing", *in IEEE international conference on utility and cloud computing*, PP.No 49-56 , 2011.
9. Miami, Florida, "Attack surfaces: A taxonomy for attacks on cloud services," in *IEEE international conference on cloud computing*, PP.No-276-279, 2010
10. Poonam Yadav, and Sujata, Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA, *In International Journal on Cloud Computing: Services and Architecture (IJCCSA)* ,Vol.3, No.3, PP.No. 25-41,2013.
11. Qiao Yan, F. RichardYu, Qingxian Gang, Jianqiang li, "Software defined networking and distributed denial of service(DDOS) attacks in cloud environment: A Survey, some research issues and challenges," *in IEEE communication Survey & Tutorial*, Vol-18, issue-1,2016
12. Naseer amara, Hang Zhiqui, Awais ali, "Cloud computing security threats and attacks with their mitigation techniques," in I*nternational conference on cyber enabled distributed computing and knowledge discovery*, PP.No. 244-252, 2017.

13. Akhilesh kumar, "Handling DDoS attacks in Cloud computing based on SDN system,"in *International journal of science computer science engineering and information technology,volume-2*, issue-2, PP.No. 62-68, 2017.
14. Vidhya V, "A review of DoS attack in Cloud computing," in IOSR journal of computer engineering, volume-16, issue-5,PP.No. 32-35, 2017.
15. Shakti Arora and Surjeet Dalal, "A variant of secret Sharing with Poly 1305," Recent development of computational intelligence, (Springer Series of computational intelligence), ISBN 978-3-03012500-4, Doi/10.1007/978-3-030-12500-4–C-CTP-05/2016.
16. Shakti Arora and Surjeet Dalal, "Hybrid algorithm designed for handling remote integrity check mechanism over dynamic cloud environment," International journal of Engineering & Technology (Scopus), vol. 7 no.2.4, pp.161-164, 2018,.
17. Shakti Arora and Surjeet Dalal, "Enhanced privacy preserving access control in the cloud," International Journal of Recent Research Aspects, vol. 4, pp. 66-70, 2016.
18. Shakti Arora and Surjeet Dalal, "Study of Integrity Based Algorithms in Decentralized Cloud Computing Environment," International Journal of Institutional and Industrial Research, vol.1, no.1, pp. 15-17, 2016.
19. Shakti Arora and Surjeet Dalal, "Novel approach for Integrity Verification in Dynamic Cloud environment," International journal of science and information security, vol.14, no. 8, 2016.

AUTHOR PROFILE

Ms. Shakti Arora, Research Scholar SRM University, Sonepat, Haryana, published more than 35 research papers, life time member of CSI, Total teachings Experience is 15 years. The research Area is Cloud security, and more than 10 papers have been published in area of cloud security, which includes one SCI and 4 Scopus publications. A patent is also filed for the cloud security domain

Dr. Surjeet Dalal, received his Ph.D. Degree in 2014 from Suresh Gyan Vihar University Jaipur (Rajasthan) and M.Tech Degree in 2010 from PDM College of Engineering, Bahadurgarh Haryana. He has completed B.Tech (Computer Science & Engineering) from Jind institute of Engineering & Technology Jind (Haryana) in 2005. He has more than nine years of teaching experience in various colleges under Kurukshetra University Kurukshetra. His current research area is Artificial Intelligence, Multi-agent system, Case-based reasoning and Cloud Computing. He has presented more than twenty papers in the national/international conferences. He has published more than thirty papers in the national and international journals. He has guided many M. Tech students for their thesis work under Kurukshetra University, Kurukshetra. He is the reviewer of many national/international journal of repute in India and Abroad. He is the professional member of various professional and research committees. He is the professional member of CSI India, IEEE New York, IETE Chandigarh and ISTE-AICTE New Delhi