International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-7, May 2020

Distinct Machine Learning Based Strategies to Detect Ddos Attack Within the Network Environment

Prabhdeep Kaur, Amit Chhabra

Abstract : In network there are different kinds of attack that impact its presentation and it might hazard security amid the transmission. The security is the serious issue in network that may hurt by these attacks. In this paper the investigation of DDOS attack in network must be handled. However, with the fast development of network technology issues related with security are offering great challenges. Security concerns like security threat and attack are disaster for both service provider and service consumer. In this paper the different procedure that are uses to recognize DDOS attack in network are considered. In this various machine learning based strategies are analyzed to detect DDOS attack in network.

Keywords: network, DDOS, authentication.

I. INTRODUCTION

Network environment is used commonly be clients and servers to access resources. The resource accessing at low cost allow many distinct users to interact with the network system. [1] Users could of distinct categories. Malicious users can hamper the performance of the network. The network based environment that is primarily considered in this literature is cloud computing. [2]The attack that is considered is distributed denial of service attack. This attack can be caused by single source or multiple sources. Due to this attack multiple packets in bulks are transmitted from source towards the sink node. As more and more packets are transmitted, network bandwidth is consumed and user is unable to access he resources offered by CSP. This means service level agreement is seriously affected by the use of this mechanism. To resolve the issue many distinct encryption mechanisms are considered in this work. As the technology advances, hardware and software becomes updated. The rectification mechanism to DDOS are being designed but execution time and reliability still is an issue that is required to be tackled. [3]Due to everlasting effects of DDOS attacks, many companies such as Amazon working towards the security based solutions. Data mining is a field that is used to tackle the issue of this attack. Layer based approach is used with input , processing and output layer. Input layers is used to store the dataset attributes.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
PrabhdeepKaur*,ComputerEngineering&Technology,Guru NanakDevUniversity,Amritsar,Punjab,India
AmitChhabra,.ComputerEngineering&Technology,Guru NanakDevUniversity,Amritsar,Punjab,India

Processing layer filter attributes and remove unnecessary data and output layer is used to print the prediction results. There are vast number of mechanisms such as random forest, regression, KNN, clustering based mechanism etc. that are used to determine abnormal patterns to detect the DDOS attack.
[4]. Considered the network based business deployment application and determines the problems if any within the system. The mechanism of DDOS attack detection considered in this system has low reliability and high execution time.

1.1 Security issues in network

In today's era, cloud based environment is commonly used to provide access to resources at cheap and best possible rates to the clients. Users intension is uncertain and hence malicious users can destroy the network along with access to resources.[5] primary usage of cloud based environment is through resource sharing. This sharing is blocked in case DDOS attack occurs within the system. This attack must be detected at early stage and prevented. [6]Security becomes an issue as DDOS attack occurs since multiple or mass packets are being transmitted by the users. This can cause bandwidth consumption and at certain time users will unable to access the resources and other services provided by service provider. This means primary concern associated with DDOS attack includes:
Lack of resource sharing

- Reliability issue
- Data Leakage

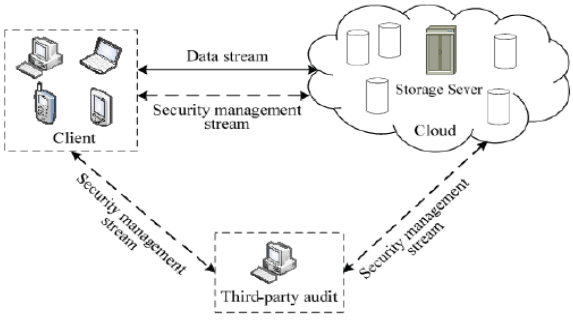

Figure 1: Data storage structure of Network

The impact of DDOS attack is primarily on the data storage of cloud computing. The structure of network storing storage is given in figure 1. Distributed property of the network allow multiple distinct users without any security procedures to interact with the resources.

Once the identity of the user is determined, CSP allow the users to access the resources. The malicious node causes the packets to transmitted again and again towards same node causing bandwidth to be consumed at rapid rate. This will cause network to be jammed and resources to be inaccessible. [7]once the resources becomes inaccessible, deadlock starts to occur. [8]this deadlock decrease the reliability of the system and popularity of certain CSP also decays. [9] To resolve the issue many researchers including post the solution including data mining strategies for detection and prevention of DDOS attacks. .

Security and privacy preserving strategies are employed within the cloud based environment so that performance of the cloud datacenters is intact. The cloud based environment suffer from many challenges. These challenges are as listed below

- Server & application access
- Transmission of data
- Secure VM
- Secure Network
- Security of Data
- Privacy of data
- Correctness of Data
- Location of data
- Availability of data
- Segregation of Data

1.2 **Network Security Challenges**

[10], [11]Some of the network security challenges that come in front of users are given below:

a. Validation: Internet usage and networks allows mass users to communicate with each other. Allowing only valid users to interact with the network is a real challenge.
b. Allowing operation: Access management is the need of the hour. The operation is in the hand of the database administrator. DBA allows the users to access the resources. To access the resources users takes the permission from the DBA. In case read only permission is given then user cannot update the data. This means only desirable operations are admissible.
c. Integrating Strategies for security: Network service provider establishes large number of policies and strategies to ensure safeguard against the malicious attack.
d. Managing distinct services provided by service providers: different security based mechanisms are applied to the services exposed to public. Primarily services such as access control and authentication is applied as security procedure.
e. Managing effective ways to ensure viability of trust: for this purpose, there are many schemes that are introduced such as offers and discounts.

[12]Network security is hampered by the threats which are common in network system. These threats are mitigated using the techniques described through the table 1.

Table 1: Types of threats and mitigation strategies.

Type of Threats	Mitigation technique
VM level Threat	IDS and IPS
Abuse and nefarious	Credit card fraud monitoring and coordination.
Loss Of Governance	No proper strategy available for handling this attack
Xml Signature Element Wrapping	Utilization of digital certificate
Browser Security	XML encryption and SOAP encryption
Network Malware Injection Attack	Authenticity check
Flooding Attacks	Intrusion detection system is used
Isolation Failure	Authentication and access control
Data Loss Or Leakage	Encrypting and protecting integrity of data
Account Or Service Hijacking	Multifactor authentication techniques

In addition threats could lead to security problems if not tackled at early stage. The security problems could hamper the overall working of the network. User data may be corrupted due to the application of attacks. Various attacks along with mitigation strategies are listed in the table 2.

Table 2: Attacks and mitigation strategies

Type of attack	Mitigation technique	Advantage	Disadvantage
Denial Of Services	Clustering based mechanism	Reduce functionality of hijackers	Time consumed more
Authentication Attacks	Access Control	Unauthorized access control	Only utilized for frequent targets
Man in the middle attack	Block Level Parity attack	Gives better prevention	Space is more consumed
DNS attack	IP address validation	Had better performance	Rerouting processing are inadequate
Network stiffing	Encryption algorithms is used	Data is secured	Much Complex
Cross site Scripting	Validating Input	Sensitive data can be secured	Violation of user credential may occur
Cookie Poisoning	Regular cookie cleanup	Removed unauthorized accessed	Must be improved for large data
Distributed Denial of service	Deadline oriented techniques	Early detection of intruder	Used more space
SQL Injection Attack	Special character elimination using buffer allocation	Eliminate intruder	More information can not be added
Side Channel Attack	Nearest Neighbor mechanism	Secured channel using nearest neighbor	Server proxy can be hacked

To optimize better results we will review some paper and find the better results to remove the security barriers. Rest of the paper is organized as follows: Section 1 provide the security concerns in network, section 2 provide the literature survey of existing techniques to derive the best possible technique for future enhancements, section 3 present the comparison table, section 4 gives conclusion and future scope.

II. BACKGOUND STUDY

This section presents the comprehensive analysis of security mechanisms based on machine learning used in network. Network security mechanisms along with distinct services provided are discussed as under

[13]Proposed a security mechanism that is Ensemble classifier which is most secure in nature. Random number generator incorporated within this encryption mechanism makes it most secured. This encryption mechanism is based upon the human ensemble classifier encoding where straight binary codes are followed to perform encryption. Result is expressed in the form of execution time and classification accuracy.

[14]Proposed a security mechanism that is based on DDOS attack detection code formation. The code security is implemented within the network system. The encryption and decryption is implemented using the networking tools. The mechanism of security ensures that space conservation and reducing execution time also.

[15]Proposed advanced encryption standards for security. This mechanism is based on sharing public key over the network. The security mechanism shares key and hence security could hamper. Malicious user can have access to private keys and encrypted text can be converted back to plain text thus enhancing DDOS attack.

[16]proposed a mechanism to ensure cyber security. The mechanism is based on tackling the attack that is multiple identity in nature. The multiple identity attack ensures that the identity of the client is hacked and abnormal activity is performed using fake identity. This can cause the problems in current account of the user. To tackle the issue KNN approach is used and result is expressed in the form of execution time and reliability.

[17]proposed a mechanism to ensure that the service level agreement is not violated. The service level agreement is insurance to clients that services that are being offered by server can be accessed by clients. The client pays for those services and hence these services must be accessible to the clients. The security of services is also ensured using DDOS attack prevention mechanism.

[18]proposed mechanism to ensure security and privacy within the cloud environment. The privacy aware mechanism is used to determine ciphertext that is being transmitted towards the destination.

Encoding the data and decoding is used using the mechanism of privacy aware mechanism.

[19]Proposed a block chaining based mechanism to ensures security of data within cloud computing. Block chaining based mechanism ensures that file being already uploaded is not uploaded again. The encryption is than applied using index base mechanism. The result is expressed using reliability and execution time.

[20]Proposed replication based mechanism in order to ensure the protection of data. Replication ensures that sensitive data can be stored within multiple location. Problem with this approach is high utilization of resources. The replication based mechanism uses parity mechanism to ensure the security among data. Reliability is the primary parameter of this research.

[21]proposed a hierarchical based security based mechanism to identify the attacker. In order to detect the attack, clusters are formed. The clusters are formed by identifying similar values within the dataset derived from kaggle. The encryption mechanism is prone with collision based key formation.

[22]Proposed elliptical encryption mechanism to ensure security among cloud environment. The encryption is based on multiple phases. First of all pre-processing mechanism is used to remove abnormalities if any within dataset. The abnormalities from within the dataset once removed, tuples from dataset is fetched. These rows are used for training and feature extraction. Hold out ratio is of 0.3 that leads to overall accuracy of 90%.

[23]proposed a mechanism to tackle DDOS attack. The DDOS attack causes the resources to be overused or not accessed by clients. The distributed attack can be caused by many distinct users. The clients cannot access resources and reliability of CSP reduces. The traffic to particular CSP is critical that is being hampered by the DDOS attack.

III. COMPARISON OF VARIOUS TECHNIQUES

Reference	Technique used	Advantage	Disadvantage
[1]	Multiple network storage with encryption	Mechanism used to ensure enhanced reliability and decrease execution time	Storage is an issue
[2]	AES based network security	Data at sender and receiver end is compared to determine validity of data.	Same server must be used to check the validity of data.
[3]	Three level protection technique	Datacenter is primary objective that is resolved using three phase mechanism	Data storage is an issue that is not resolved in this literature.
[4]	Block chain based access control	Security of data is an issue that is resolved using this literature.	Security becomes problems as more and more user interact with the system.
[5]	Memory replication mechanism	In case server is failed data can be recovered effectively.	Heavy storage demand exists that is not resolved.
[6]	Hierarchal framework	Data analysis becomes critical since source and destination are affected by DDOS attack	Space conservation is an issue not considered within this literature.
[7]	Elliptic Curve Digital Signature Algorithm (ECDSA)	Storage space is conserved along with privacy of information.	Execution time is high during encryption and decryption of data.
[8]	chaos based encryption strategy	Privacy and confidentiality of data is maintained.	Backup server can be further enhanced by considering space conservation mechanism.

This section provides the in-depth into the security mechanisms that are considered within network environment. The environment considered in the literature includes datacenter and virtual machines. The security is primarily hampered through DDOS attack. In this attack multiple distinct machines sends packets towards clients. The bulk packets jam traffic and clients unable to access resources. This will degrade the performance of cloud service provider. To tackle the issue, interpolation based mechanism can be used.

IV. RESULTS

DDOS attack will be the one in which one node takes the identity of other node.

The overall performance goes down by the application of DDOS attack. In order to resolve the problem Euclidean distance mechanism is merged along with Interpolation. Euclidean distance used to find the neighbours of the node being analyzed. In case there exist only one neighbour of current node then DDOS attack is detected. The Euclidean distance is used to check the location of the DDOS node.

The overall time consumption of simulation is achieved to be better as compare to existing approach.

V. CONCLUSION AND FUTURE SCOPE

This work presents the security mechanisms that are considered against the attacks. The most common attack that is discovered is DDOS attack. The distributed denial of service attack is most frequent attack that hamper the performance of the network. Many encryption based mechanisms are commonly employed to tackle the issue. But execution time reliability of the considered mechanisms is issue. To tackle the issue, in future interpolation based mechanism can be used. In this mechanism hold out ratio can be varied in order to obtain enhanced performance. The rectification of DDOS is primary objective in future endeavors.

REFERENCES

1 X. Tan et al., "Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm," Sensors, vol. 19, no. 1, p. 203, Jan. 2019, doi: 10.3390/s19010203.
2 N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE Commun. Surv. Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019, doi: 10.1109/COMST.2019.2896380.
3 Z. Liu, Y. Cao, M. Zhu, and W. Ge, "Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 4, pp. 1098–1108, Apr. 2019, doi: 10.1109/TIFS.2018.2870828.
4 S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, and A. Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," EURASIP J. Wirel. Commun. Netw., vol. 2013, no. 1, p. 271, Dec. 2013, doi: 10.1186/1687-1499-2013-271.
5 R. J. Hyndman and Y. Fan, "Sample Quantiles in Statistical Packages," Am. Stat., vol. 50, no. 4, p. 361, Nov. 1996, doi: 10.2307/2684934.
6 M. Aamir and S. M. A. Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," J. King Saud Univ. - Comput. Inf. Sci., Feb. 2019, doi: 10.1016/j.jksuci.2019.02.003.
7 S. Behal and K. Kumar, "Trends in Validation of DDoS Research," Procedia Comput. Sci., vol. 85, pp. 7–15, 2016, doi: 10.1016/j.procs.2016.05.170.
8 A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," Comput. Secur., vol. 31, no. 3, pp. 357–374, May 2012, doi: 10.1016/j.cose.2011.12.012.
9 C. Wang, T. T. N. Miu, X. Luo, and J. Wang, "SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 3, pp. 559–573, Mar. 2018, doi: 10.1109/TIFS.2017.2758754.
10 M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.
11 M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.
12 R. Zuech, T. M. Khoshgoftaar, and R. Wald, "Intrusion detection and Big Heterogeneous Data: a Survey," J. Big Data, vol. 2, no. 1, p. 3, Dec. 2015, doi: 10.1186/s40537-015-0013-4.
13 F. S. de Lima-Filho, F. A. Silveira, A. M. B. Junior, G. Vargas-Solar, and L. F. Q. Silveira, "Smart-Detection: Feature selection algorithm." Code Ocean, 2019, doi: 10.24433/CO.0280398.v2.
14 A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
15 R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," IEEE Commun. Mag., vol. 40, no. 10, pp. 42–51, Oct. 2002, doi: 10.1109/MCOM.2002.1039856.
16 S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison, "An Inter-Domain Collaboration Scheme to Remedy DDoS Attacks in Computer Networks," IEEE Trans. Netw. Serv. Manag., vol. 15, no. 3, pp. 879–893, Sep. 2018, doi: 10.1109/TNSM.2018.2828938.
17 W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data," IEEE Access, vol. 6, pp. 7234–7243, Nov. 2018, doi: 10.1109/ACCESS.2017.2772294.
18 K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," Comput. Secur., vol. 65, pp. 344–372, Mar. 2017, doi: 10.1016/j.cose.2016.10.005.
19 N. Vlajic and D. Zhou, "IoT as a Land of Opportunity for DDoS Hackers," Computer (Long. Beach. Calif)., vol. 51, no. 7, pp. 26–34, Jul. 2018, doi: 10.1109/MC.2018.3011046.
20 M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," Security and Communication Networks, vol. 9, no. 16. John Wiley and Sons Inc., pp. 3724–3751, 10-Nov-2016, doi: 10.1002/sec.1539.
21 Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm," IEEE Access, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.
22 A. Marzano et al., "The Evolution of Bashlite and Mirai IoT Botnets," in 2018 IEEE Symposium on Computers and Communications (ISCC), 2018, vol. 2018-June, pp. 00813–00818, doi: 10.1109/ISCC.2018.8538636.
23 H. H. Jazi, H. Gonzalez, N. Stakhanova, and A. A. Ghorbani, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," Comput. Networks, vol. 121, pp. 25–36, Jul. 2017, doi: 10.1016/j.comnet.2017.03.018.

AUTHORS PROFILE

Prabhdeep Kaur (Btech in computer science and engineering from GNDU regional campus Gurdaspur and Mtech in CSE from GNDU,Amritsar)

Amit Chhabra (Assistant Professor at GNDU , Amritsar. Areas of specialization in Parallel and Distributed Computing)