e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

DETECTION AND PREVENTION MECHANISMS FOR DDOS ATTACK IN CLOUD COMPUTING ENVIRONMENT

Ms. Mohanasundari M[*1], Aathish B[*2], Kavin Kumar M [*3], Dharshan G[*4]

[*1] Associate Professor, Department of Computer Science And Engineering, Velalar College Of Engineering and Technology, Erode, Tamil Nadu, India

[*2,3] Student, Department of Computer Science and Engineering, Velalar College of Engineering And Technology, Erode, Tamil Nadu, India

ABSTRACT

The prominence and utilization of Cloud processing are expanding quickly. A few organizations are putting resources into this field either for their own utilization or giving it as an assistance to other people. One of the consequences of Cloud advancement is the development of different security issues for both industry and customer. One of the approaches to getting Cloud is by utilizing Machine Learning (ML). ML procedures have been utilized in different ways to forestall or identify assaults and security holes on the Cloud. In this paper, we give a Systematic Literature Review (SLR) of ML and Cloud security strategies and procedures. We broke down 63 significant investigations, and the aftereffects of the SLR are classified into three principles research regions: (I) the various kinds of Cloud security dangers, (ii) ML methods utilized, and (iii) the presentation results.

In addition, conveyed forswearing of administration (DDoS) and information protection are the most widely recognized Cloud security regions. And the most applied measurement is a valid positive rate, and the least utilized is preparing time. Ultimately, from 20 datasets discovered, KDD and KDD CUP datasets are the most utilized among pertinent investigations.

Keywords: Cloud processing, Cloud security regions, J48, SVM, KDD Dataset.

I. INTRODUCTION

Distributed computing is a mechanical development that offers the offices, stage, and programming of data innovation as Internet administrations. It is viewed as the transformation of a durable dream called computing for Use,'' and it is, in effect, step by step embraced by associations as private, public, or mixture Clouds. Its fundamental goal is to allow clients to utilize and pay for what they need, promising on-request benefits for their product or framework needs. Although Cloud registering is viewed as a significant and positive IT foundation shift, much security work is as yet expected to limit its deficiencies. Since a significant measure of individual and corporate data is put in the Cloud server farms, those Cloud security issues and weaknesses should be identified and forestalled. The partner editorial manager organizing the audit of this original copy and endorsing it for distribution was Ines Domingue.

II. METHODOLOGY

CLOUD COMPUTING SECURITY: Distributed computing security or, all the more just, cloud security includes an expansive arrangement of approaches, advancements, applications, and controls used to ensure virtualized IP, information, applications, administrations, and all the more extensively, data security. And It furnishes clients with abilities to store and handle their information in outsider information centers. Now Multiple Organizations operate the cloud in a wide range of administration prototypes (with abbreviations like SaaS, PaaS, and IaaS) and sending models (private, public, half and half, and local area).

DDOS MITIGATION: DDoS relief is a bunch of procedures or devices for opposing or alleviating the effect of appropriated disavowal of administration (DDoS) assaults on networks connected to the Internet by securing the objective and transfer organizations. DDoS assaults are a steady danger to organizations and associations

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

by undermining administration execution or closing down a site completely, in any event, for a brief time frame. The main thing to do in DDoS moderation is to distinguish typical conditions for network traffic by characterizing "traffic designs", which is vital for danger identification and alarming. DDoS relief additionally requires distinguishing approaching traffic to isolate human traffic from human-like bots and captured internet browsers. The interaction is finished by looking at marks and inspecting various properties of the traffic, including IP addresses, treat varieties, HTTP headers, and JavaScript footprints.

PRIVACY: Security is the capacity of an individual or gathering to disconnect themselves or data about themselves and accordingly articulate their thoughts selectively. When something is private to an individual, it usually implies that something is innately unique or delicate to them. The space of protection, to some extent, covers security, which can incorporate the ideas of proper use and insurance of data. Security may likewise appear as important honesty. The right not to be revealed to unsanctioned intrusions of protection by the public authority, partnerships, or people is essential for some nations' security laws and, now and again, constitutions.

III. RELATED WORKS

Rohit Bhadauria et.al., has proposed Cloud Computing holds the possibility to dispense with the prerequisites for setting up of high-cost processing foundation for the IT-based arrangements and administrations that the business employments. It vows to give an adaptable IT design, open through the web for lightweight, convenient gadgets. This would permit many-crease expansion in the limit or abilities of the current and new programming. Since these server farms might lie on any side of the world past the span and control of clients, there are diverse security and protection moves that should be perceived and dealt with.[1]

Umer Ahmed et.al. has proposed But Cloud figuring (CC) is on-request availability of organization assets, mainly information stockpiling and handling power, without extraordinary and direct administration by the clients. CC has arisen as a bunch of public and private data centers that offer the customer a solitary stage across the Internet. Edge figuring is a developing processing worldview that brings calculation and data stockpiling closer to the end clients to develop reaction times and extra bandwidth further. Versatile CC (MCC) utilizes dispersed figuring to pass on applications to mobile phones.[2]

Adel Abusitta et. al. proposed that the most recent couple of years have seen the capacity of helpful cloud-based Intrusion Detection Systems (IDS) in identifying refined and obscure assaults related to the intricate engineering of the Cloud. In a pleasant setting, an IDS can counsel other IDSs about dubious interruptions and settle on a choice utilizing a collection calculation. Notwithstanding, undesired postponements emerge from applying accumulation calculations and, furthermore, from holding on to get input from counseled IDSs. These impediments render the choices produced by existing helpful IDS approaches ineffectual progressively, subsequently making them unreasonable.[3]

P. Achilleos et. al. has proposed Cloud registering offers an adaptable pay-more only as costs arise model for provisioning application assets, which empowers applications to scale on request dependent on the current responsibility. By and large, however, clients face the single merchant lock essentially, passing up on favorable circumstances for ideal and versatile applications sending across numerous mists. A few clouds displaying dialects have been created to help multi-cloud asset the executives, yet they need an all-encompassing Cloud board, all things considered, and stages.[4]

Rafael Moreno-Vozmediano et.al., has proposed Automated asset provisioning strategies to empower the execution of versatile administrations by adjusting the accessible assets to the help interest. This is fundamental for lessening power utilization and ensuring QoS and SLA satisfaction, particularly for those administrations with severe QoS necessities as far as inactivity or reaction time, for example, web workers with high traffic load, information stream preparing, or constant colossal information investigation. Versatility is regularly carried out in cloud stages and virtualized server farms through auto-scaling components. These

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

settle on mechanized asset provisioning choices dependent on the worth of explicit foundation as well as administration execution measurements.[5]

IV. PROPOSED METHODOLOGY

It is not difficult to work on their proposed work by adding more components or empowering it to identify more kinds of assaults. The help vector machines are the proposed work which is more productive and precise when joined with j48 we propose a mixture calculation for quicker, effective, and more exact outcomes for the distinguishing proof of DDoS assaults with the fundamental component choices.

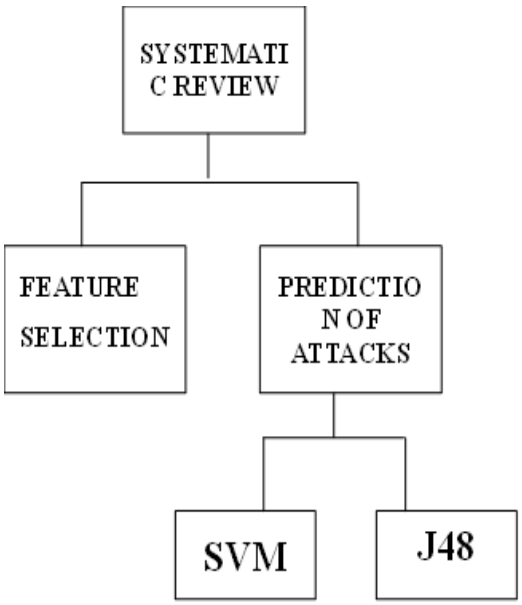

Figure1: Workflow

FEATURE SELECTION

A portion of the essential provisions of the DDOS assaults should be chosen with the goal that the recognizable proof of the assaults can be distinguished a portion of the boundaries incorporate the SRC/DST, and diverse kinds of assaults can be recognized.

CONFUSION MATRIX

In the disarray network, the upsides of every cycle of genuine positive and genuine negative, bogus positive and bogus negative are determined and can be distinguished by the SVM calculation and these strategies are utilized to ascertain the absolute number of examples and the A disarray grid is a procedure for summing up the exhibition of a characterization calculation. Grouping exactness alone can be misdirecting on the off chance that you have an inconsistent number of perceptions in each class or then again on the off chance that you have multiple classes in your dataset.

PREDICTION OF ATTACKS USING SVM AND J48

The expectation of assaults in the dos and the many administrations can be distinguished by the SVM and j48 calculations which are quick and effective in recognizing the different sorts of assaults as the outcome will be climate the distinguished occurrences are ordinary or inconsistency this calculation will recognize the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

precision forecast esteem which is more essential to recognize the assistance assaults in the organization and cloud climate.

V. EVALUATION

For each RQ, the results of this SLR will be given and tended to in the accompanying subsections. Addendum A shows all papers gathered with their IDs and titles from the 63 papers we have gathered, we conclude that 11 Cloud security issues are tended to and explored. These are peculiarity location, assault discovery, classification of information, information protection, DoS, DDoS, interruption recognition (ID), malware, protection safeguarding, security, and weakness identification. The number of examination papers in each cloud security region and the recurrence of the space, just as the rate. Location of oddities includes discovering designs in the information that don't relate to expected conduct. Oddity discovery is significant on the grounds that information inconsistencies are fundamental and frequently basic data that can be followed up on in an expansive scope of uses. Despite the fact that A4-A5 include research on irregularities, they zeroed in on conduct inconsistencies. One of the top Cloud security regions talked about in our example of papers is information protection.

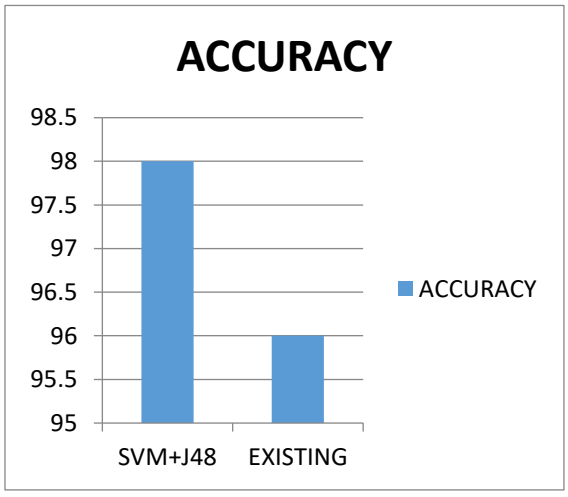

Figure 2: Comparison Between Proposed and Existing System.

VI. CONCLUSION

We carried out a systematic literature review to analyze ML techniques used in Cloud security. The review investigated relevant studies that answered 3 RQs; Cloud security area, type of ML techniques used, and the accurate estimation of the ML model. Overall, our conclusions are summarized as follows: RQ1 findings are the 11 Cloud security areas identified; anomaly detection, attack detection, privacy preservation, security, vulnerability detection, the confidentiality of data, data privacy, DDoS, DoS, and intrusion detection (ID). DDoS and data privacy are analyzed the most, with a 16% frequency of usage and 14% respectively. RQ2 counted 30 ML techniques used, some used as hybrid and others as standalone. Identification of correctly classified instances and incorrectly classified instance are all segmented and the accuracy for each segmentation is identified.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:05/May-2022 Impact Factor- 6.752 www.irjmets.com

ACKNOWLEDGEMENTS

I convey my heartfelt indebtedness to my guide**, Ms. Mohanasundari M,** for her esteemed guidance, constructive criticism, inspiration, and constant encouragement during the completion of research work and to the Head of Department **Dr. S. Jabeen Begum** for his continuous encouragement during research work. Also, I would like to appreciate the moral support of my team partners. I am very thankful again to all people who helped me during this project.

VII. REFERENCES

[1] H. Tabriz chi and M. Kuchaki Rafsanjani, ‘‘A survey on security challenges in cloud computing: Issues, threats, and solutions,’’ J. Supercomput., vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi: 10.1007/s11227-020- 03213-1.Gyusoo Kim and Seulgi Lee, “2014 Payment Research”, Bank of Korea, Vol. 2015, No. 1, Jan. 2015.

[2] Abusitta, M. Bellaiche, M. Dagenais, and T. Halabi, ‘‘A deep learning approach for proactive multi-cloud cooperative intrusion detection system,’’ Future Gener. Comput. Syst., vol. 98, pp. 308–318, Sep. 2019, doi: 10.1016/j.future.2019.03.043.

[3] P. Achilleos, K. Kritikos, A. Rossini, G. M. Kapitsaki, J. Domaschka, M. Orzechowski, D. Seybold, F. Griesinger, N. Nikolov, D. Romero, and G. A. Papadopoulos, ‘‘The cloud application modelling and execution language,’’ J. Cloud Comput., vol. 8, no. 1, p. 20, Dec. 2019, doi: 10.1186/s13677-019-0138-7.

[4] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, ‘‘A survey on the security of cloud computing,’’ in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019, pp. 1–7, doi: 10.1109/CAIS.2019.8769497.

[5] R. Kumar and R. Goyal, ‘‘On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,’’ Comput. Sci. Rev., vol. 33, pp. 1–48, Aug. 2019, doi: 10.1016/j.cosrev.2019.05.002.

[6] L. B. Bhajantri and T. Mujawar, ‘‘A survey of cloud computing security challenges, issues and their countermeasures,’’ in Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC), Dec. 2019, pp. 376–380, doi: 10.1109/I-SMAC47947.2019.9032545.

[7] K. Vijayakumar and C. Arun, ‘‘Continuous security assessment of cloud based applications using distributed hashing algorithm in SDLC,’’ Cluster Comput., vol. 22, no. S5, pp. 10789–10800, Sep. 2019, doi: 10.1007/s10586-017-1176-x.

[8] A. Singh, U. Chandra, S. Kumar and K. Chatterjee, "A Secure Access Control Model for E-health Cloud," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 2329-2334.

[9] W. Ahmad, S. Wang, A. Ullah, Sheharyar, Z. Mahmood, "ReputationAware Trust and Privacy-Preservation for Mobile Cloud Computing," in IEEE Access, vol. 6, pp. 46363-46381, 2018.

[10] W. Jiannan, W.Xiaojie, L. Nan, Y. Guomin, M. Yi, "A PrivacyPreserving Fog Computing Framework for Vehicular Crowdsensing Networks" (2018). Faculty of Engineering and Information Sciences, vol. 6, pp. 43776-43784, 2018

[11] M. Zekri, S. E. Kafhali, N. Aboutabit and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, 2017, pp. 1-7.