A Novel attack detection and encryption Framework for Distributed Cloud Computing

[1]Prasanna Balaji Narasingapuram, [2]M. Ponnavaikko

[1]Research Scholar, Computer Science Engineering/Information Technology, Bharath Institute of Higher Education and Research (BIHER), Chennai, India.
prasannabalaji.narasingapuram@gmail.com.

[2]Provost, Bharath Institute of Higher Education and Research (BIHER), Chennai, India.
ponnav@gmail.com

Abstract:

Cloud Computing has advanced as another worldview in which clients can use on-request services, as indicated by their necessities. Nonetheless, security concerns are essential obstructions to a more extensive reception of clouds. Recently conceived ideas that clouds presented, for example, multitenancy, asset sharing and redistributing, make new difficulties for the security research. DDoS (Distributed Denial of service) attack is the greatest danger to the cloud since it influences the availability of services. The objective of this exploration is to build up a security service calculation that lessen the time intricacy, increment the security level and improves the presentation in different factors. The presentation consequence of this proposed calculation is investigated by contrasting it and other existing cryptographic calculations. This exploration work centers primarily around plan a data security calculation to decrease the encryption and decoding time and attack discovery in cloud environment. A progression of investigations were performed and the outcomes exhibit that this methodology can effectively recognize and relieve DDoS attacks from an assortment of known and obscure sources. The Optimised results like accuracy, precision and recall produced by KNN(k=4) compare with other models for this research work. This model has given the optimal solutions.

Keywords: Encryption, Decryption, attack detection, NaiveBayes Classifier, DDOS attack, Third Party Auditor(TPA),KNN, botnet, sigmoid capacity based strategic relapse method, Randomforest, Cloud Service Provider (CSP),Cloud Security.

1 INTRODUCTION

The cloud is the assortment of asset pool which contains number of assets and services which can be accessed by the quantity of services gave by different service providers. The services gave by the service providers can be accessed by the clients upon arrangements. The client must concur the service arrangements to access the services. Upon understanding the client will be given with interesting personality which is utilized to recognize the client character. The client should clear the security check to access the service. Data security is a basic region in cloud computing environments [1]. Cloud has no restrictions, and the data can be truly positioned anyplace in any data place over the organization geologically conveyed. The clients are compelled to utilize the stage and infrastructure gave by a similar service supplier, and henceforth the service supplier knows where the clients data are found and have full access to the data. This situation of cloud raises a few issues with respect to clients secret data [9].

Securing delicate data is central for data proprietors. In the function, if such data are unveiled, the data proprietor needs to confront the outcomes. Having data with various affectability levels, it is a great idea to order the data dependent on its affectability level. The term staggered in this paper alludes to the diverse security groupings dependent on the affectability of the data. Staggered security or various degrees of security is to order data and ensure the characterized data by furnishing security at various levels beginning with access authorization dependent on security freedom which is trailed by data encryption, integrity check, and log examination. Among the four essential security estimates expressed above, in this paper, characterization followed by encryption is talked about comprehensively. A DDoS is a DoS that utilizes a high number of hosts to make the attack much more troublesome. A Distributed Denial of Service attack is a co-ordinated attack by a malevolent user(s) on an asset by immersing it with constant high-rate authentic solicitation packets in a brief span of time which eventually brings down the asset and renders it futile for real clients. It is an attack by various sources on a solitary objective framework [7].

Numerous works have attempted to address DDoS before, however DDoS attacks stay a significant security issue; recognition and protection is hard, particularly with regards to exceptionally disseminated executions. A large portion of the works send a solitary highlight apply the responsive system against DDoS traffic. Rather than this methodology, a dispersed guard instrument conveys various focuses for various assignments through the

organization to ensure the casualty hub/organization. Along these lines, sending at various focuses in the organization is a significant thought for making a precise channel to isolate great traffic from attack traffic, and finding an effective strategy to channel. As of now, there is no solid collaboration system among switches and the casualty hub to distinguish and secure against the attack in an appropriated conspire. Henceforth, giving an agreeable protection component can be a huge improvement here.

The rest of the paper is organized as follows: Sect. 2 explains related works to cloud DDoS attack. Section 3 discusses proposed method used to find potential features of DDoS attack. Section 4 illustrates the proposed method with an example based on dataset. Section 5 we conclude the paper.

2.RELATED WORKS

Various techniques have been contemplated that are explicitly intended to deal with DDoS attacks. These approachs center around both identification and counteraction, however every framework works from a broadly alternate point of view. Exploring these various techniques considers a more noteworthy comprehension of how DDoS identification and avoidance can be progressed.

Plan proposed in [3] utilizing Third Party Auditor, hash work and. In this plan, the outsider reviewer (TPA) is considered in dynamic and plays out all the calculations and checks. It is realized that we can't completely trust on TPA's, that it can utilize the data of DO for own money related benefit. Another improvement field in proposed conspire [13] is breaking the much straightforward than factoring [14]. Plan proposed in [15] is dependable to acquire access control and confidentiality of data. In this methodology, the creator scrambles data through mystery keys and these keys are simply perceived to DO and comparing data clients. The scrambled documents are put away at CSP. During the correspondence among CSP and the client, data are additionally scrambled through one-time private meeting key which is shared among CSP and the client through the altered Diffie-Hellman convention. This plan gives full data security however there is a key comparing to each record and client yet in certain applications, documents and clients might be huge in numbers. Along these lines, there may have an enormous number of keys.

In [19] additionally surveys a few strategies for botnets identification, presents an approach to characterize the procedures of botnet recognition, and features the parts of such strategy investigation with subjective exploration plan. The creators characterize conceivable future methods of improving the strategies of botnet discovery and distinguish the relentless exploration issues, which stay open. In [2] depicts the development of DDoS attacks and their place in present day half breed attacks and dangers. In [1] clarifies in more detail the idea of DDoS attack, its impact on cloud computing, and important worries that must be thought of while choosing protection systems for DDoS, closing with the proposal to pick a utilitarian, clear, lightweight, and exact answer for forestall DDoS attacks. The identification of DDoS attacks with the guide of connection investigation shapes the premise of examination in [12]. Their methodology depends on a closest neighbors traffic grouping with connection examination. It improves the grouping exactness by misusing the relationship data of preparing data and lessens the overhead coming about because of the thickness of preparing data.

3. CLOUD INFRASTRUCTURE DOS ATTACK IDENTIFICATION (CIDAI)

3.1.Anomaly Detection

An interruption recognition framework is ordinarily used to distinguish malignant digital attack conduct on an organization while checking and assessing the everyday exercises in an organization or PC framework to recognize security dangers or dangers [11]. Various explores has been led in the zone of network safety with the capacity of recognizing and forestalling digital attacks or interruptions. Mark based organization interruption discovery is one of the notable systems utilized in the digital business [14]. This framework considers a known mark and has seen far and wide appropriation remembering business accomplishment for ongoing time. Then again, the inconsistency based methodology has advantage over the mark based methodology for recognizing concealed attacks, including the capacity to distinguish obscure or zero-day attacks [10]. This methodology screens network traffic and discovers attack standards of conduct by investigating the pertinent security data. Different data mining and AI strategies are utilized to dissect such security occurrence designs for settling on valuable choices [15]. The fundamental disadvantage of the oddity based methodology is that it might create high bogus alert rates as it might order the beforehand concealed framework practices as irregularities [10]. In this manner, restricting the bogus positive paces of an interruption location framework must be a main concern [13]. Hence, an AI based powerful identification approach is expected to limit these issues. The zone of AI is ordinarily considered as a part of man-made reasoning, which is firmly identified with computational insights, data mining and data science, and basically centers around making PCs to gain from data [9]. It has solid connections to numerical speculations, techniques, measurable investigation, streamlining, and different true application spaces in the field. Hence, in the territory of cybersecurity, AI is a kind of data-driven technique in which understanding the crude security data is the initial step to fabricate a clever security model for making forecasts about future occurrences. In spite of the fact that, the affiliation examination is mainstream in AI methods to construct rule-based clever systems [1], in this work, we fundamentally center around grouping learning procedures [4] that are

commonly used to assemble a prescient model by using a given preparing dataset. For example, to construct a data-driven prescient model, a few mainstream procedures, for example, the likelihood based credulous Bayes classifier, hyperplane-based help vector machines case learning-based k-closest neighbors, the sigmoid capacity based strategic relapse method, just as rule-based characterization like choice trees have been utilized [9]

3.1. Prevention of DDoS Attack

This sort of attacks can wiped out by utilizing following methodologies, for example, channel based methodology, signature based methodology, firewalls. Channel based methodology: Flow level channel is utilized to identify the low rate DoS attack. Low rate DoS attack which progressively increment the traffic rate and attack the organization have. Stream level channel which blocks the DoS attacks [5]. In PC organization, the traffic of the organization is observed alongside signature design. The attacks design is contrasted and help of mark database. The database walls one in or more number pre-characterized marks. In the event that the deals coordinate with database signature traffic it will find a way to block the attacks. Firewalls are one of the strategies for Intrusion Prevention System. The principle thought of utilizing firewall inside the environment to force try procedure and safeguard affiliation state data for real clients both inside and furthermore remotely and not to forestall high volume DoS/DDoS style attacks.

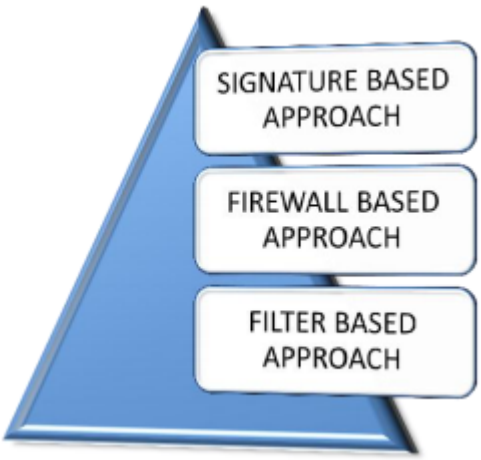

Fig.1 Approaches to Attacks

3.2. Machine Learning Approaches

In this work dataset derived from UCI repository.[16,17]. Cyber security dataset containing nine different network attacks on a commercial IP-based surveillance system and an IoT network. The dataset includes reconnaissance, MitM, DoS, and botnet attacks. This work implemented in python 3.8.0.

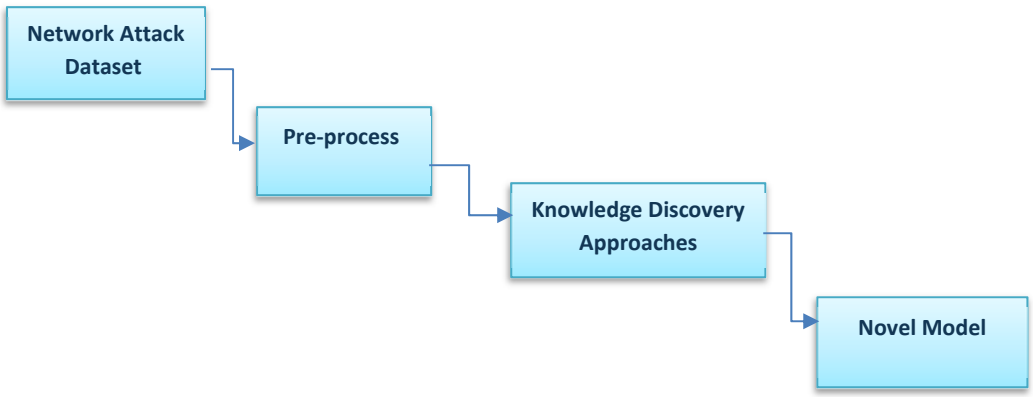

Figure 2. Proposed System

The above diagram represents that the proposed system for applying the Artificial Intelligence Algorithms in given dataset.

4. RESULTS AND DISCUSSIONS

4.1. **CIDAI Process**

This work has been executed in a private cloud called eucalyptus cloud. For examining the CPU, principle memory and circle use at client and cloud service supplier sides, the reenactment programming Eucalyptus‖ has been introduced in Linux operating framework. In addition, two bunch level segments are conveyed at the head-hub of one group. At long last, every hub with a hypervisor was utilized with a Node Controller (NC) for controlling the hypervisor. We have played out our testing in the Amazon EC2 cloud environment, utilizing m1.medium example types [3]. In the current setting, example implies a virtual machine running on the Amazon EC2. We contrast our proposed convention CSAP and the comparative model customary RBAC and ITRBAC conventions.

Table 1 Parameter Settings

Name	Intel Xeon E5
Number of core	1
Speed	2114Mhz
Specification	Xeon(R)
Memory Size	3840 Mbytes
Memory Frequency	102.2 MHz

Figure 2 demonstrates the attacks dispersion in the test sessions for some clients and the detection threshold that CIDAI processes for every client in the preparation stage. Compare with other model CIDAI had good results.

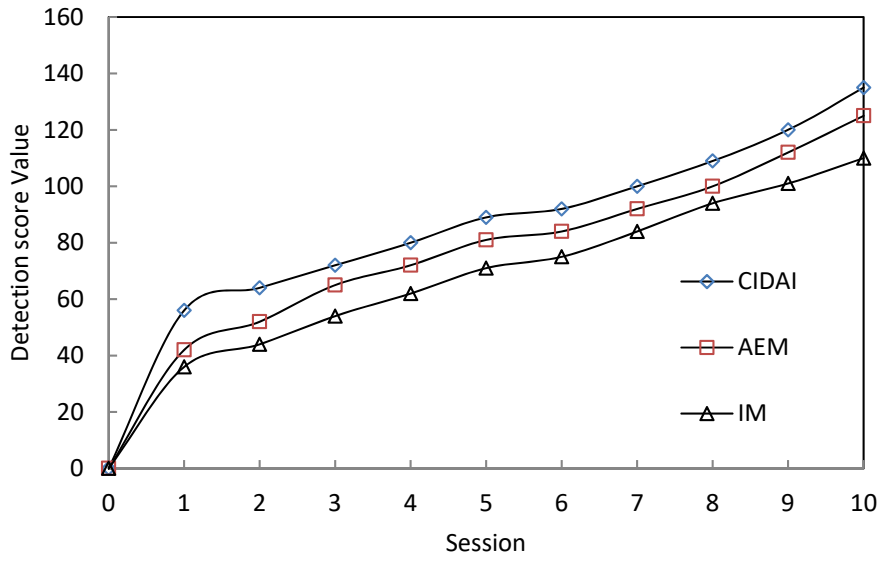

Figure 3: Detection Score Value

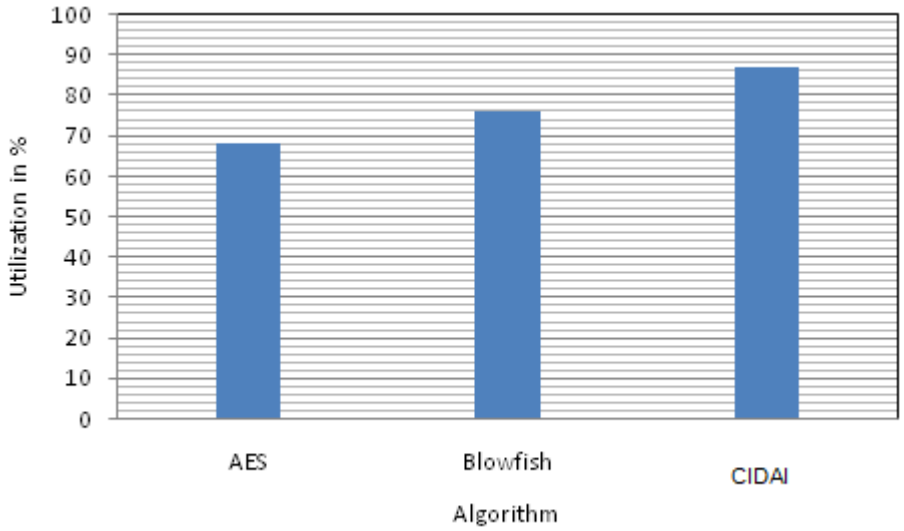

Figure 4: Service Utilization

The figure 3 shows the comparative results on service utilization and the result shows clearly that the proposed method has produced higher service utilization than other methods. The latency ratio is the time delay between the encryption and decryption. It depends on the speed of the algorithm and how long it takes for the process.

4.2. Machine Learning Approaches

The below table represents that the accuracy, precision and recall values of the various Machine Learning approaches NaiveBayes, Support Vector Machine, Instance Based Classifier k=2, Instance Based Classifier k=4,and Random Forest approaches.

Table 2: Accuracy, Precision and Recall values of the ML Approaches

List of Approaches	Accuracy	Precision	Recall
NaiveBayes	73.91	74.77	0.76
Support Vector Machine (SVM)	76.77	73.12	0.73
Instance Based Classifier k=2	77.15	71.27	0.74
Instance Based Classifier k=4	80.27	81.89	0.83
Random Forest	72.89	72.77	0.71

Naïve Bayes classifier has been produced 73.91% of accuracy value and 74.77% of precision value and 0.76 of recall value. Support vector machine classifier has been produced 76.77% of accuracy value and 73.12% of precision value and 0.73 of recall value. Instance based classifier (if k=2) has been produced 77.15% of accuracy value and 71.27% of precision value and 0.74 of recall value. Instance based classifier (if k=4) has been produced 80.27% of accuracy value and 81.89% of precision value and 0.83 of recall value. Random Forest classifier has been produced 72.89% of accuracy value and 72.77% of precision value and 0.71 of recall value.

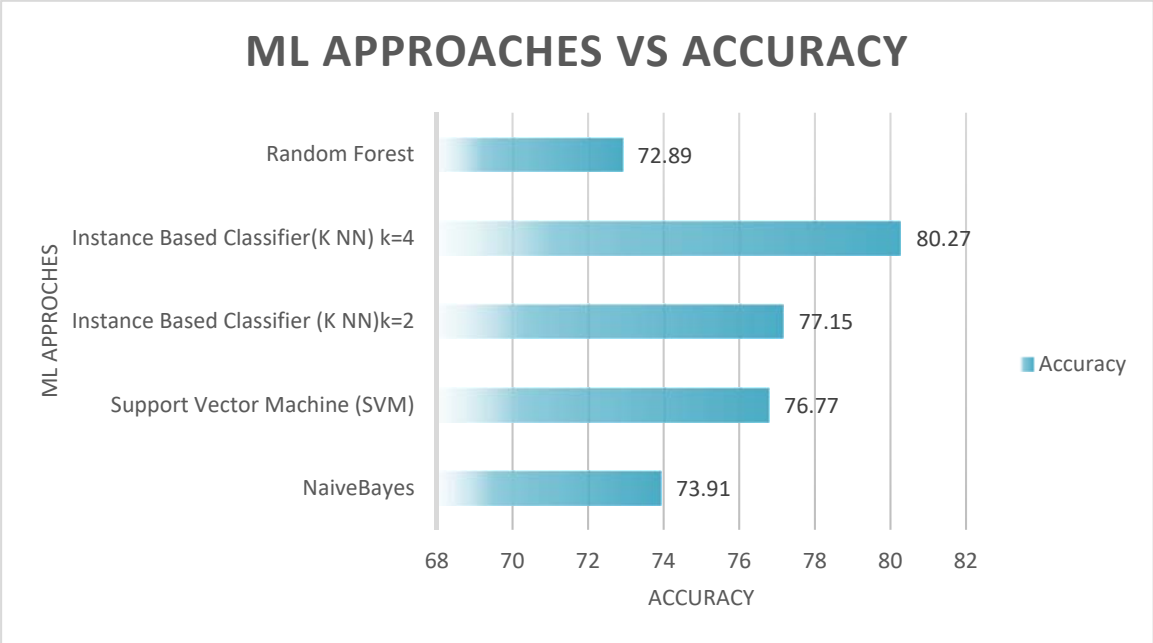

Figure 5: ML Approaches Vs Accuracy

The above diagram shows that the Random forest is holding 72.89% of accuracy level, Instance Based Classifier(K=2) is holding 77.15% of accuracy level, Support Vector Machine (SVM) is holding 76.77% of accuracy level, and NaiveBayes Classifier is holding 73.91% of accuracy level. These classifiers have below 80% of accuracy levels. The one only Instance Based Classifier has above 80% of accuracy level.

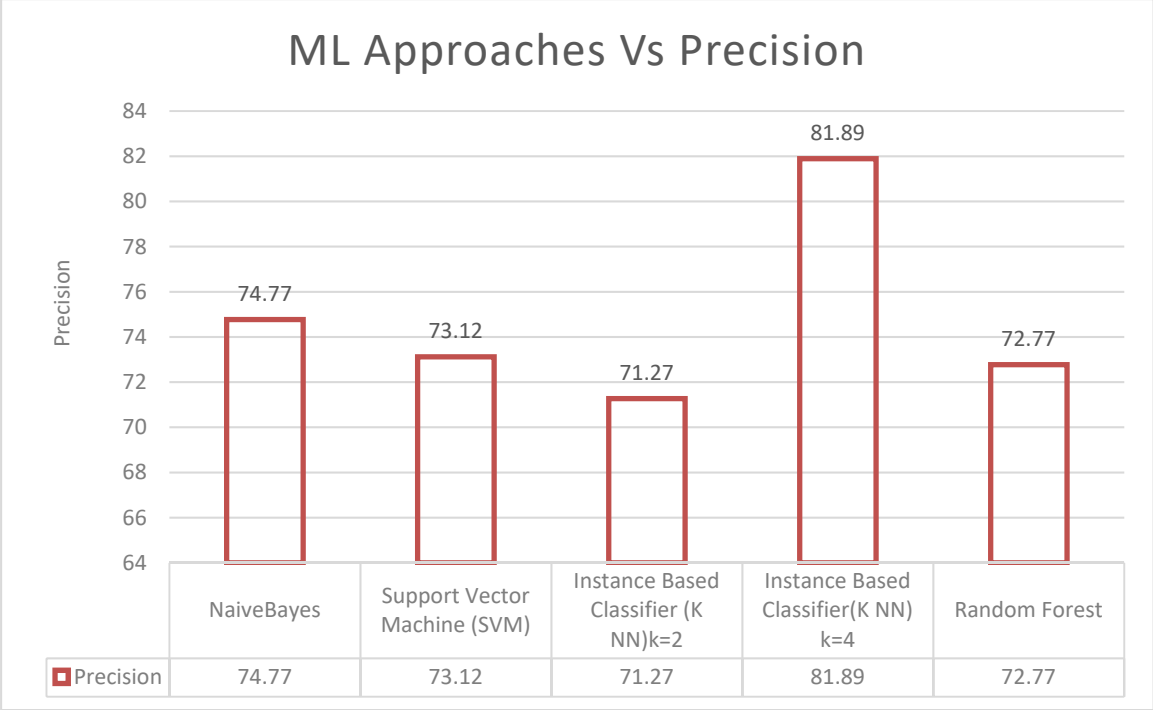

Figure 6: ML Approaches Vs Precision

The above diagram represents that the various ML approaches of this dataset. NaïveBayes gives 74.77% of precision value, Support Vector Machine Gives 73.12% of Precision value, Instance Based Classifier has 71.27% of precision value while applying the k value is 2, Instance Based Classifier has 81.99% of precision value while applyin ght k value is 4, and Random Forest is 72.77% of precision value. The Lazy classifier only has highest precision value which is 81.89% rest of the machine learning approaches have the precision values from 71.27% to 74.77%.

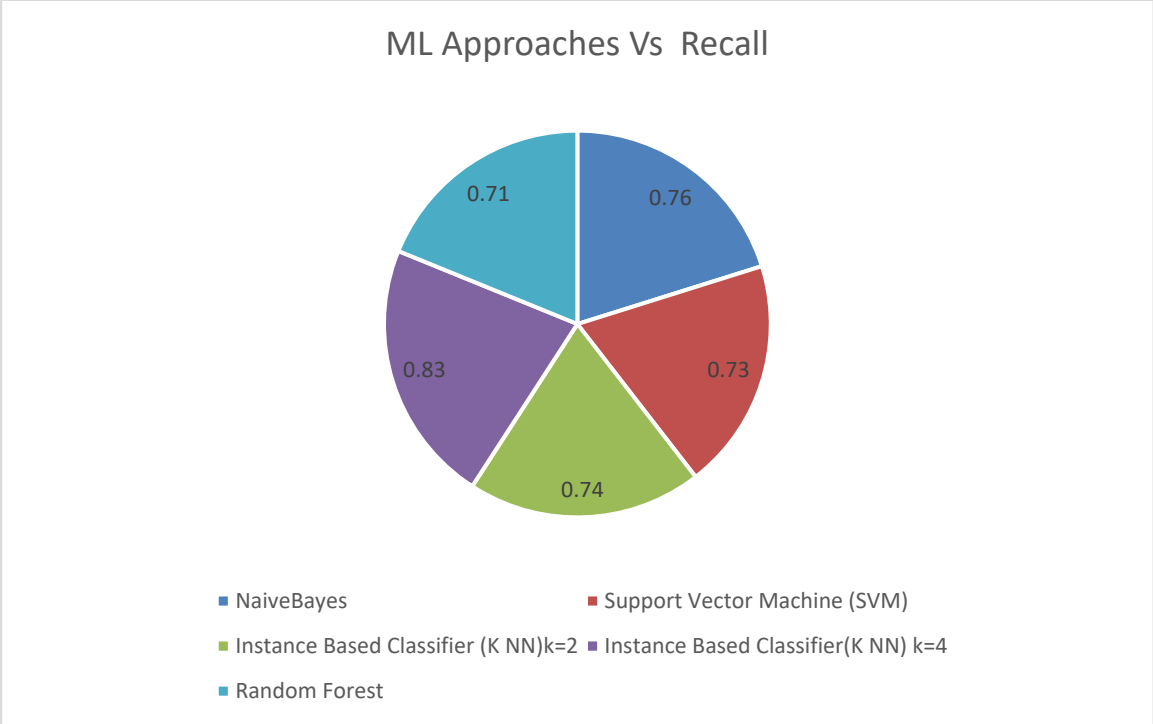

Figure 7: ML Approaches Vs Recall

The above diagram represents that the various ML approaches of this dataset. NaïveBayes gives 0.76 of recall value, Support Vector Machine Gives 0.73 of recall value, Instance Based Classifier has 0.74 of recall value while applying the k value is 2, Instance Based Classifier has 0.83 of recall value while applying the k value is 4, and Random Forest is 0.71 of recall value. The NaiveBayes, SVM, KNN(if k=2) and RandomForest approaches have the recall value from 0.71 to 0.76. the KNN (If k=4) classifier has highest recall value which is 0.83.

5. CONCLUSION

In this paper, a crossover CIDAI calculation was talked about in the cloud environment and measures the subsequent exhibition. The technique gets the client demand and distinguishes the data being submitted. At that point the technique performs service taking care of and gets the outcome from the service. The outcome has been encoded utilizing the CIDAI calculation and a similar will be decoded to the opposite end in the cloud environment. It was discovered that the proposed calculation has improves the presentation of the data security. This examination shows an outline of DDoS attacks, explicitly transfer speed flooding and association flooding, location plans lastly research issues and difficulties have been introduced. Likewise, an examination among current recognition strategies and an approach to advise the manager about causing DDoS attack has been given. The Optimised results like accuracy, precision and recall produced by KNN(k=4) compare with other models for this research work. This model has given the optimal solutions.

Reference

[1] L. Badger, T. Grance, R. Patt-Corner and J. Voas, “Cloud computing synopsis and recommendations (draft), nist special publication 800-146”, Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).
[2] U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, “Cloud based secure and privacy enhanced authentication & authorization protocol”, Procedia Computer Science, 22, (2013), 680-688.
[3] T. Acar, M. Belenkiy and A. Küpçü, “Single password authentication”, Computer Networks, 57(13), (2013), 2597-2614.
[4] G. Wang, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, Computers & Security, 30(5), (2011), 320-331.
[5] C. I. Fan and S. Y. Huang, “Controllable privacy preserving search based on symmetric predicate encryption in cloud sSDEMage”, Future Generation Computer Systems, 29(7), (2013), 1716-1724.
[6] D. W. Chadwick and K. Fatema, “A privacy preserving authorisation system for the cloud”, Journal of Computer and System Sciences, 78(5), (2012), 1359-1373
[7] S. Ludwig. Cloud 101: What the heck do IaaS, PaaS and SaaS companies do? VentureBeat, 2011, https://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/ , Accessed on 20th August 2017.
[8] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, M. K. Khan. A Review on remote data auditing in single cloud server: Taxonomy and open issues. Journal of Network and Computer Applications, Vol. 43, 2014, p.121-141.
[9] Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. 2016, 67, 147–165.
[10] T. Z. R. B. L. Zecheng He, “Machine Learning Based DDoS Attack Detection From Source Side in Cloud,” 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017.
[11] M. E. M. Wesam Bhaya, “A Proactive DDoS Attack Detection Approach,” Journal of Next Generation Information Technology, pp. 36-47, 2014.
[12] K. P. Devi, “A Security framework for DDoS Detection in MANETs,” Telecomminication and Computing, pp. 325-333, 2013.
[13] Bikram Khadka, Chandana Withana, Abeer Alsadoon, Amr Elchouemi, 2015. Distributed Denial of Service attack on Cloud Detection and Prevention. School of Computing and Mathematics, Charles Sturt University, Sydney, Australia Hewlett Packard. 2015 International Conference (pp. 1-5). IEEE.
[14] Suresh K.C., Haripriya K. and Kruthika S.R."Cooperative Multipath Admission Control Protocol: A Load Balanced Multipath Admission Policy", Research Journal of Biotechnology, Vol. (Special Issue II), August (2017)
[15] Qiao Yan, F. Richard Yu, Qingxiang Gong, Jianqiang Li, 2015. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. 2015 IEEE Communications Surveys & Tutorials (pp. 2-4). IEEE.
[16] https://archive.ics.uci.edu/ml/datasets/Kitsune+Network+Attack+Dataset.
[17] Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai, 'Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection', Network and Distributed System Security Symposium 2018 (NDSS'18)