





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.

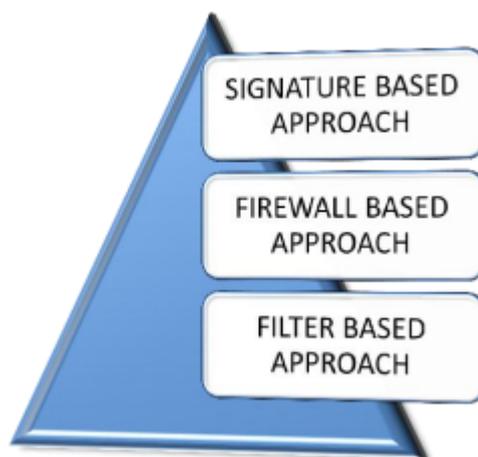


Fig.1 Approaches to Attacks

### 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.

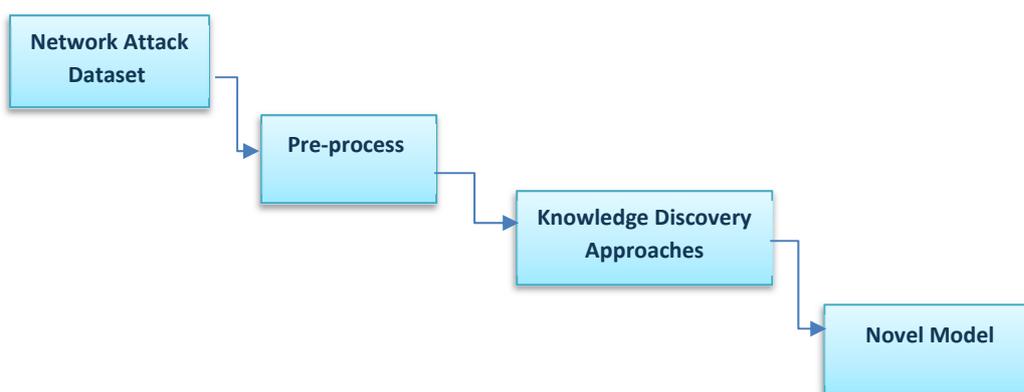


Figure 2. Proposed System

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 Eucalyptusl 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.

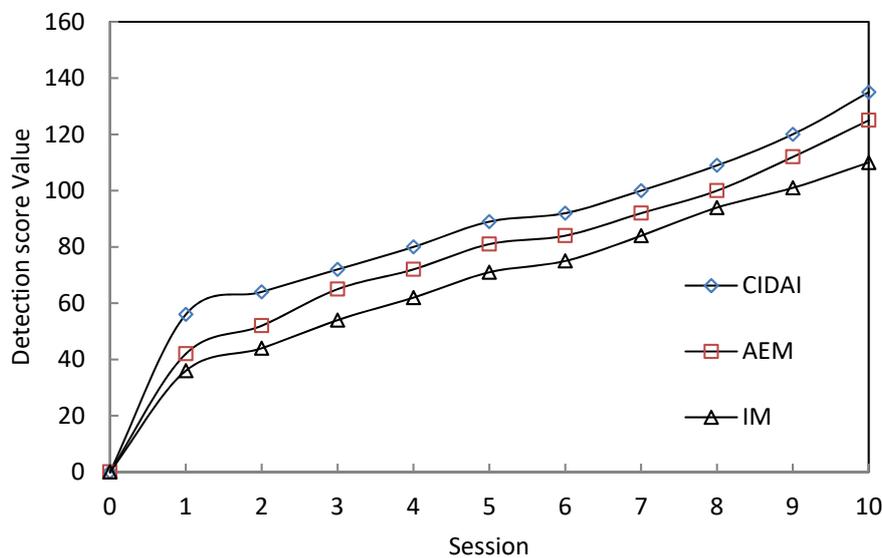


Figure 3: Detection Score Value

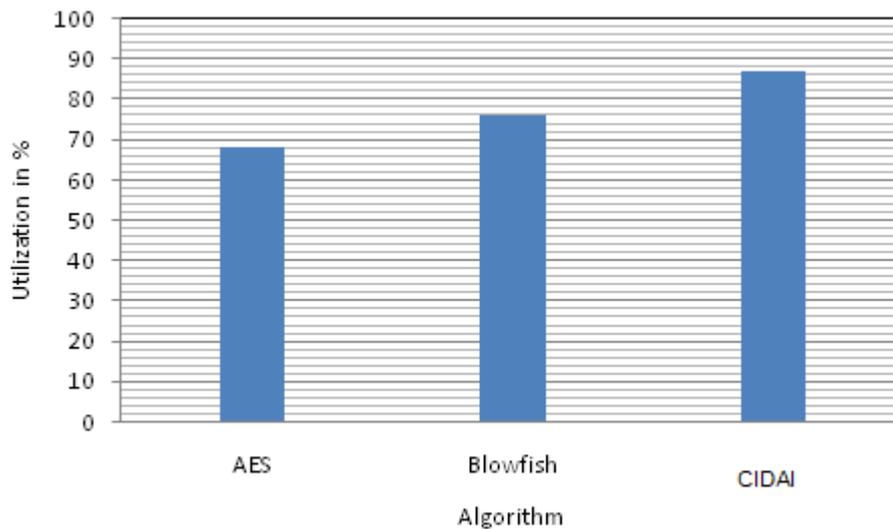


Figure 4: Service Utilization

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.

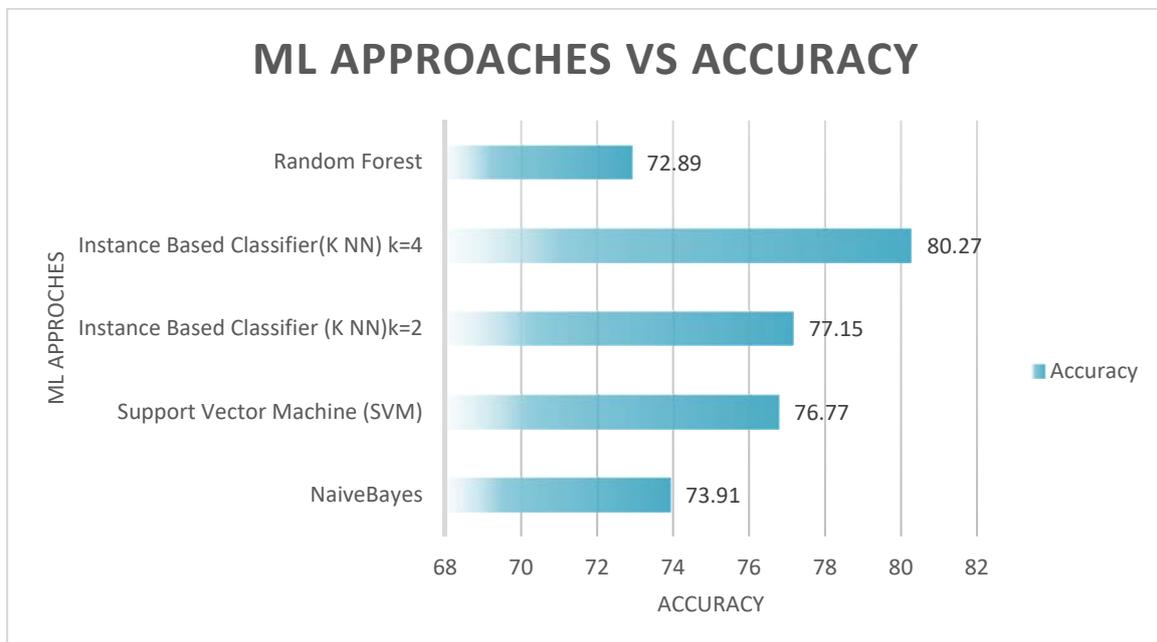


Figure 5: ML Approaches Vs Accuracy

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.

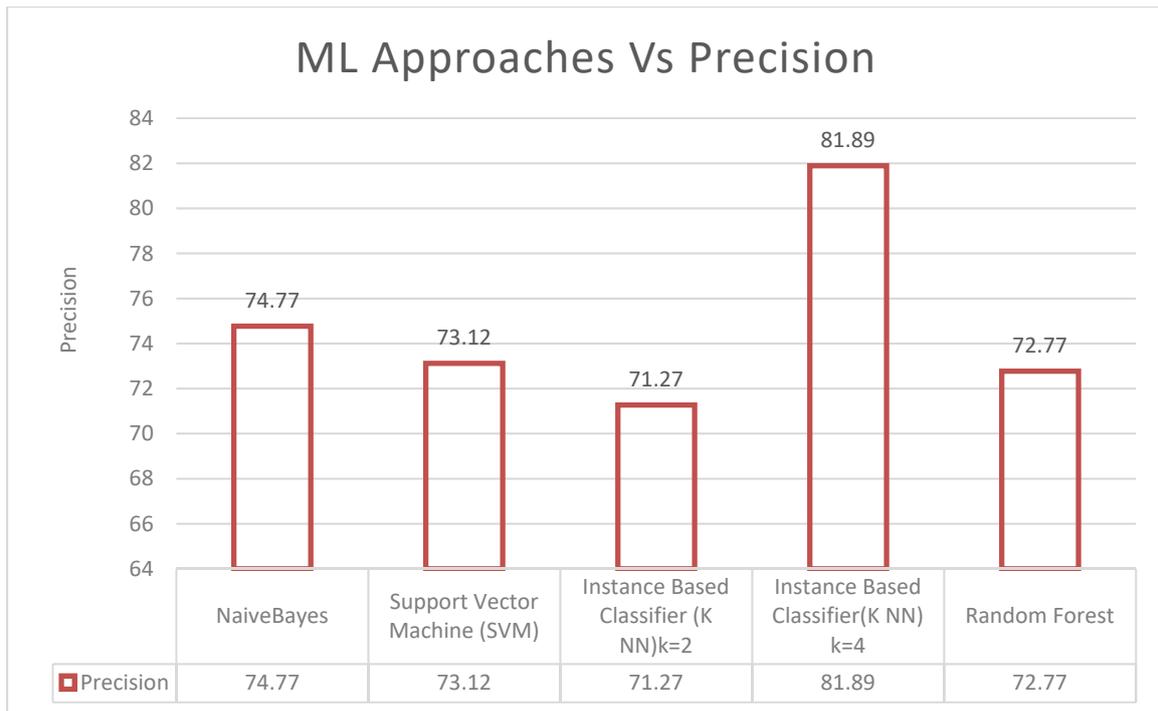


Figure 6: ML Approaches Vs Precision

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%.

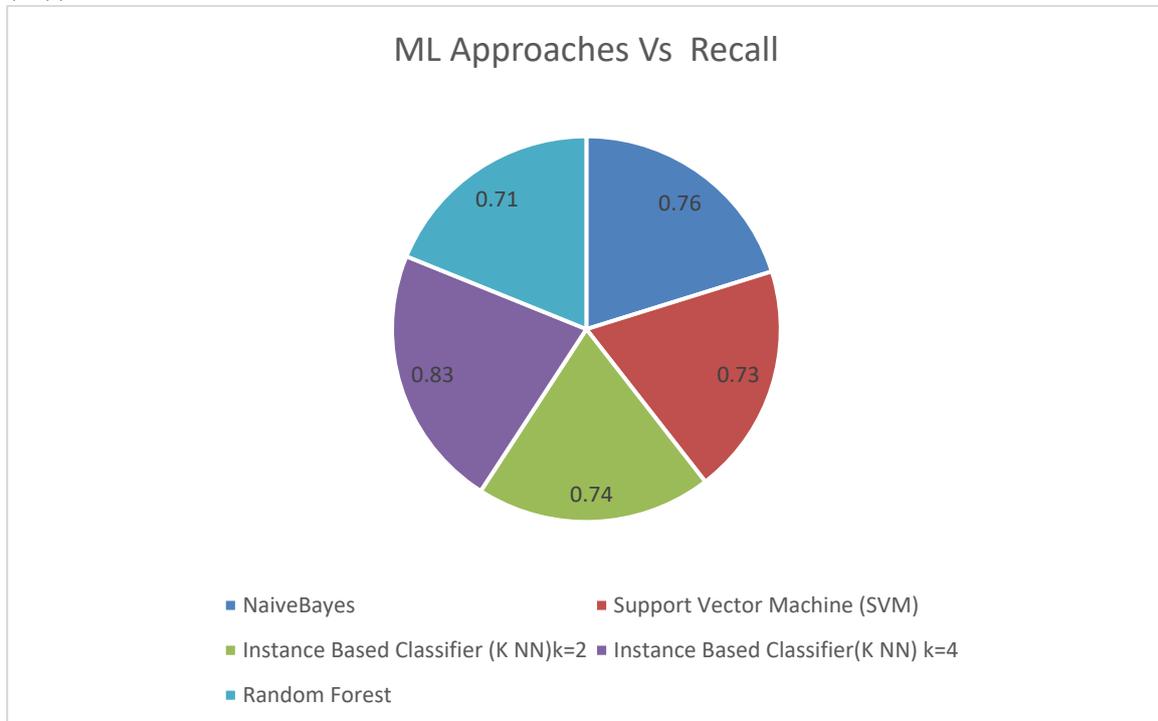


Figure 7: ML Approaches Vs Recall

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. Ghafour, 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," *Telecommunication 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)*