DDOS ATTACK SECURITY IN THE DIGITAL COMPUTING AND NETWORK MANAGEMENT SERVICES

T. Kuppuraj, M. Mohankumar*

Abstract

Digital computing is an Information Technology tool for providing end-users with more adaptability, lower maintenance and fewer construction costs for computationally efficient virtual server on demand resources. Such services are managed and distributed over the network by different planning organisations and the protocols standards known for networking. The threats that cause significant injury and impact on the cloud output seem to be the most frequent such as Distributed Denial of Service (DDoS). In a DDoS attack, the attacker typically use vulnerable corrupted devices (known as monsters) to allow huge packets of data from such previously captured monsters to be sent from a network by using temporary or permanent software vulnerabilities. This can occupy a large part of the target cloud technology's bandwidth utilization or take a lot of servers processing time. Therefore in this paper, Statistical classifier algorithm based signing detection methods (SA-SDM) for the reduction of the DDoS attacks risk. Statistical classifier algorithm reduces the attacks occurring in the cloud and network services. This, along with signing detection methods, provides a technique to find signing attacks automatically and effectively for DDoS replay attack.

Keywords: Distributed Denial of Service (DDoS), Digital Computing, Signing Detection Methods, Signing Attacks.

I. INTRODUCTION

Taking into account of Information Technology advancement, many organizations have started to find ways for minimizing IT expenses and defeating economic decline. [1] Cloud storage is between many new technologies where people have to charge only for the use of providers without any cost for the rest of the purchase of smart objects. [2] It can be found, that cloud takes their business via network, anytime and anywhere with only a desktop, notebook, mobile device is needed with the network interface. [3] These extensible facilities are offered by server virtualization in computing. The position of computing resources, a strong high performance of cloud computing network for solving diverse and complex science and mathematical issues, was created by cloud services. [4] The model of the cloud becomes a leading forum for domestic and foreign users because of its accessibility and versatility. [5] Computing means a type of device on the network that offers a shared amount of money, including bandwidth utilization, memory, storage and application software. [6] The services can easily be supplied to customer with little management and less network costs on request over the Network. [7] It can also be used as a personal, open, local or resources based cloud. Some of the main obstacles that technology faces today are to reduce the number of organisations that can take up the cloud unconditionally. [8] DDoS is a kind of malicious attack causing significant cloud service difficulty. The DDoS attack happens when the capacity or services of a network connect typically to one or even more application server. [9] A network is the product of several processes. This threat often results from the flood events of the target computer with congestion by several infected computers. [10] Distributed DDoS attacks, attempts to make a device or corporate network inaccessible to its designated users. [11] The service provider and intelligence analysts have made considerable solutions to tackle this problem for years but the intensity and

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

effect of attacks continues to rise. [12] DDoS is an assault in which a goal, other than a network, a database, or another system component, is attacked by several infected computer networks and denies access to a targeted object. The influx of news content, link demands or deformed packages in the targeted system causes it to stop working or get crashing, and therefore prohibits authorized customers or devices from using the system. [13] Numerous entities of risk including single computer criminals to criminal organizations, government bodies are responsible for DDoS attacks. Even valid applications to goal programs can produce DDoS-like effects in some cases, often associated with bad programming, incomplete updates or typically insecure structures. [14] The attacker starts using susceptibility on a personal computer and becomes the DDoS expert for typical DDoS attacks. [15] The threat control machine detects and gains power from the other compromised machines by either harming vulnerabilities or by overriding associated with traditional. Three kinds of DDoS attacks are possible. Network-or parametric attacks overwhelm product with usable message flooding capacity. Specification assaults of physical network goal or tier communication protocol by overwhelming intended assets with network defects. And operating system targets the systems or servers overloading with huge amounts of device requests. The flooding of the goal packages leads to an application proxy. The (DDoS) assault, with more than a desktop targeting, an offender in a systematic fashion. This research includes the implementation of DDoS attack detection with machine-learning algorithm. The issue of computer vision detecting attacks is not fresh to research. Even if technologies of signature verification are able to recognize threats from an already learned documents, the technologies of learning algorithms would understand from the guideline pattern of internet traffic and extract relevant substantially different from the benchmark pattern. Signature detection systems are successful when anomalies are observed and unidentified and fresh threats are observed. The information flow of the threat is erratic. DDoS attacks could build relevant corporate threats with long-term consequences. Consequently, knowing the threats, vulnerabilities and costs involved with DDoS attacks is essential to IT and protection professionals and their management. The complete architecture of DDoS attack is shown in figure1.

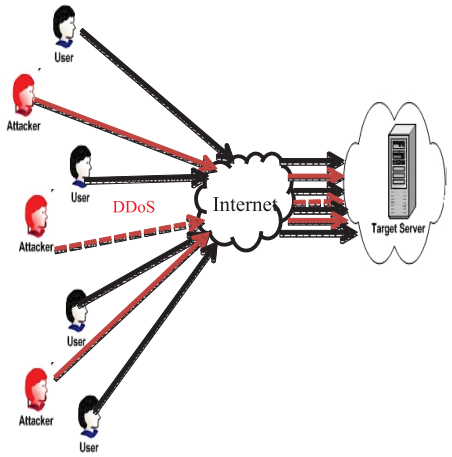


Figure1. Complete flow of DDoS attack

The paper suggests statistical classifier algorithm based on signing detection methods (SA-SDM) can be used for the reduction of the DDoS attacks' risk. The part 2 of the paper provides insights about background studies and the part 3 discusses on the Statistical classifier algorithm and how it reduces the attacks occurring in the cloud and network services. This, along with signing detection methods, provides a technique to find signing attacks automatically and effectively for DDoS replay attack. The Part 4 validates the results. Part 5 concludes the research.

II. BACKGROUND STUDY ON DDOS ATTACK

This section discusses several works that has been carried out by several researchers; N.Ch.S.N. Iyengar et al [16] introduced application denying and distributed denial of service attacks in the private cloud to prevent authorized users from accessing the services and proposed a fuzzy logic-based protective mechanism that could be used to identify

suspicious cartons using limited amount and to take appropriate anti-DDoS action. An intensive study was also carried out on various forms of DDoS attacks and current security techniques.

Bing Wang et al [17] propose a DDoS mitigated threat framework incorporates several forms of network controlled devices to enable for a fast and accurate attack response, as well as different modelling structure. Designers suggest a controller design detection accuracy framework in order to adapt the current design. It could address the change question of the database. The findings of analysis confirm that the design tackles the problem of protection by this new service model quickly and successfully and, utilizing modern world data traffic, the detection accuracy strategy can efficiently monitor numerous attacks.

Adnan Rawashdeh et al [18] suggest an approach to anomalous identification of intrusions in the hardware level to prevent DDoS behaviours among virtual servers. In order to identify the congestion swapped among virtual servers, the suggested technique is adopted through the genetic computer program, which incorporates Particle Swarm optimization process with the neural network. Performance evaluation and outcomes of the suggested protocol identify and classify cloud-based DDoS attacks with minimal misalarms and high precision of identification.

Monowar H. Bhuyan et al [19] explore scientifically many primary metrics of knowledge, such as entropy of Hartley, Shannon entropy, entropy of Renyi, widespread entropy, the variance of Kull-Back – Leibler and generally calculated the distance in the capacity of both low-grade and high-grade cyber-attacks. These measures could be used to the development of organizational traffic information features and an adequate metric allows the creation of an efficient model for identification of both low and high speed DDoS attacks. The reliability and efficacy of each DDoS variable is demonstrated via the MIT Lincoln Lab, CAIDA and TUIDS DDoS databases.

Keisuke Kato et al [20] developed an effective tracking system for DDoS attacks and it is considered as one of the most complicated jobs in information security. DDoS attacks the network communication where client sends various boxes to the destination server via numerous cracked bots. The server has been survivors of the assaults from several companies and/or government agencies. With such an attack it is extremely difficult to control the crackers as they only give commands from some other network through several bots and then depart bots rapidly after executing the order.

Yang Xiang et al [21] determine the difference among normal users and attack data with 2 additional data metrics, such as the standardized uncertainty metrics and the data distance metric, to detect lower-rate DDoS attacks. The simplified entropy metrics can measure a number of nodes earlier than that of the standard Shannon measure (three hops earlier). The process of monitoring the distance to measure outputs the famous Kullback – Leibler divergence method (six hops earlier, while ordering)is used, since it can obviously increase the dispute resolution range and achieve an optimum sensor performance.

Fang-Yie Leu et al [22] propose a disbursed detection method based on remote monitoring architectural design for the identification of Dos/ DDoS attacks through a scientific method comparing the standard and recent message metrics are allowed to address the discrimination against a DDoS attack. It gathers all message statistics for resource IPs in order to produce their standard deviation of packets. This method, according to experimental data, can detect possible assaults by DDoS.

Bin Jia et al [23] propose a DDoS attack detection system based on a multi classification multi-hybrid

conventional educational learning and development of a probabilistic valuation analysis of the result to create the network of detection. Test results reveal that TNR, correctness and accuracy are outstanding for the detection technique. The classifier used in the proposed method has good DDoS detective efficiency by comparing the three algorithms, SVD and SVD (Random Forest), Closest Neighbour and packing, which include the classification part.

Jisa David et al [24] propose improved tracking by means of flow-based assessment of dispersed denial of services based on a strong entropy process. The methodology of the estimation algorithm is used as system because the behaviour of users could change over in time. In comparison with conventional entropy calculations, quick randomness and stream-based results demonstrate significant reductions in time to maintain a positive detection precision. Data transmission is evaluated and fast demand entropy is determined per stream.

Junho Choi et al [25] proposed a method of integrating HTTP GET for the flood between MapReduce and DDOS attacks for rapid cloud-based detection system. This technique allows for efficient and precise HTTP-GET floods identification of the targeted system. The time required for Quality assessment contrasts snicker identification with specific pattern detection for attack apps. The method implemented is stronger than the Snort sample detection technique because of a short response time with rising traffic. Based on the statistical survey, Statistical classifier algorithm based signing detection methods (SA-SDM) are used for the reduction of the DDoS attacks risk. Statistical classifier algorithm reduces the attacks occurring in the cloud and network services. This, along with signing detection methods, provides a technique to find signing attacks automatically and effectively for DDoS replay attack.

III. STATISTICAL CLASSIFIER ALGORITHM BASED SIGNING DETECTION METHODS

Statistical classifier algorithm based signing detection methods (SA-SDM) are used for the reduction of the DDoS attacks risk. Statistical classifier algorithm reduces the attacks occurring in the cloud and network services. DDoS attacks are designed to prevent valid users from having direct connections to the layer of the open systems. Framework is helpful to understand the kinds of attacks to interact and address internet connection's unique structures. Two key ways of causing DDoS attacks in the Web are presently available. The other is to give the victim malfunctioning packets. The second approach consists of a perpetrator attempting one or both. Typically, DDoS attacks are inspired by many factors. Evaluating the motivations of the hacker helps to avoid the attack and give time for response. Important targets of businesses that are usually irritated by men are likely with poor technical knowledge. The threats are generally young hacker's enthusiasts who want to demonstrate their experimental and apprenticeship functionality. This class of aggressors is typically triggered strategically to target rising vital parts of some other community.

3.1. SIGNING DETECTION METHODS

By authority to monitor and by finding patterns that fits the documents of common threats, the sign-based identification devices can detect interference. A sign of an offense describes the critical activities necessary to carry out the attacks and how they are to be carried out. In addition, only threats that signs have been saved in the system are detected. The documents must be continuously updated for tracking purposes. Just as possible risks are frequently issued, potential hazards to the partners are material obtained, increasing the need for lead time. This method is the most useful against the corrected patterns of behaviours. Due to its capacity to detect new attacks, signing detection has attracted the attention of researchers. The identification is

focused on network data description. The components of the system comply with the present actions.

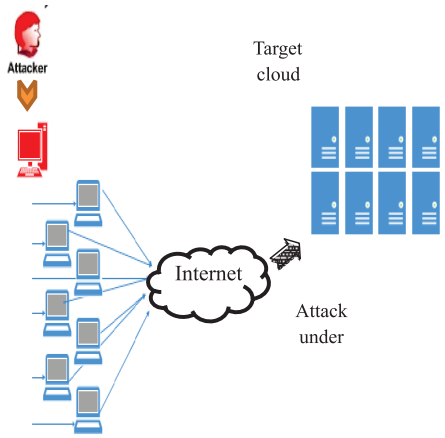


Figure 2. Signing Detection methods

Then the occurrence in sign based detection is acknowledged or otherwise activates. The primarily operates recognized by network management can be trained or taught. The major benefit of sign based detection over signature-based motors is that if the local traffic trends are not observed, a novel assault where no stamp exists can be identified. Risk management and measurement offer multiple methods in which health issues can be classified and approximated, potential defence mechanisms estimated and their efficiency reduced. A detailed study of the impetus behind the release of a DDoS attack needs to take place to formulate an efficient defence strategy. In consideration of possible attack strategies, attack incentives and reasons for attack, the prevention method of attack must be established. This is perhaps the most popular opportunity to release DDoS attacks by freshman hackers who use a few other techniques to get knowledge or just for fun. Such form of threat can, moreover, always be identified in the beginning and communication from the victim system is easy to distinguish. A good cyber rules and effective security system are valuable to discourage these activities. This is a popular setting for conducting DDoS assaults on commercial entities for competing parties having business and monetary market advantage. Throughout this case however, expert cheaters are recruited and the assault is very risky, insistent and difficult to reduce. These on-going threats disturb public infrastructure and harm prestige through daily sales. Many dissatisfied consumers, upset staff, or dissatisfied hackers launch attacks for retribution. The offender can subsequently request Paying for stopping the DDoS benefit attack. That's just another significant motivation for a strong DDoS assault by hacker groups, army or criminal groups aimed at stopping regular activities. Such an attack requires high expertise and professional attackers to paralyze the everyday internet operations and critical services produced in the country causing massive socio-economic losses. In particular, the attacker's goals are on Resources, banking and financial institutions, government services and web databases, state-owned entities, telecommunications and internet network providers, transportation and electricity infrastructures, national healthcare firms, etc... are accessible both explicitly and implicitly. Other prevalent subsidies may be, except for these primary motives, hackers, who want to develop reputation and image in the Internet, government-led or personal-security testing, arbitrary lightning assaults, self-induced unplanned threats, etc... There are various DDoS Attack Resources that would quickly be accessed and then used to initiate a network attacks instantly, for various operational platforms. It actively encourages attackers to play toward local enterprises with network attacks. Attempts started, furthermore, are always seen as innocent or quickly linked back to take some court action against the offender with very little planning or technological knowledge. Cloud infrastructure is essentially the aggregation of resources. Protecting a cloud service requires protecting it against the limitations in the digital network and software incorporation. DDoS is an appropriate term to describe a community of attackers rather than a specific form of network connection. The DDoS attack is intended to exploit vulnerabilities in convolutionary in different networks.

3.2. STATISTICAL CLASSIFIER ALGORITHM

In this section statistical classifier algorithm is a probabilistic classifier, which claims a parameter quality is not influenced by other parameters. This hypothesis is known as class secession. Tree of choice is yet another of the different classifiers , well-known and used extensively. This methodology is focused on a limited tree structure, recursive technique. The tree based is sometimes referred to as a statistical classifier and can be used for classification. The Statistical classifier algorithm is defined as a main decision tree system by authors from the machine learning platform and now which was possibly the most commonly used computer teacher in operation. The assessment of grouping data sets represents the distance between both the vector group and piece of data. Sign detection is mostly achieved using machine learning methods. Individuals are very interested in addressing weak points in body of knowledge detection systems by many remote monitoring investigators. Experiments indicate that Statistical classifier algorithm has greater stability and programs based on a remote monitoring model have shown that Statistical classifier algorithm is the best detection system and the best training time. Therefore, in the proposed model, Statistical classifier algorithm technique is used to find attacks by DDoS. The complete flow of proposed SA-SDM is shown in figure3.

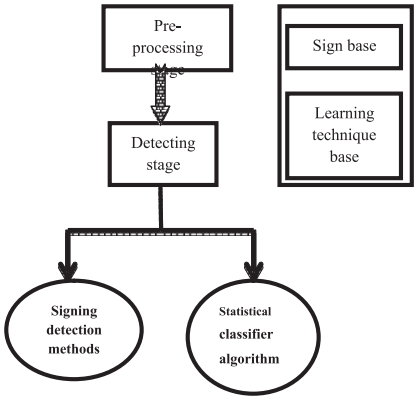


Figure3. The complete flow of proposed SA-SDM

As illustrated in figure pre-processing system strategies are defined by eliminating unwanted details with really detection rate relation in some formats. For example, signature-based detection coincides with both the guidelines in the existing knowledge of a specific network incident and effectively activates common threats. One benefit of using such technology is that there is chance of upgrading the knowledge and understanding quickly before setting the constitution in place. It includes data collection (located in learning techniques) relevant to valid user behaviour, and then by use of a computer learning techniques to evaluate whether or not this client is lawful. The objectives is to accomplish through the implementation of the proposed model are listed below. They now have following objectives: minimal price of computing, higher rate of recognition, DDoS service identification in network surroundings, excellent performance.

Statistical classifier algorithm is used to evaluate our performance, because sign detection is used in software known as snort. Snort is free software using sign based attack detection technology. It is popular and can also be run on many platforms. In fact, it is continuously updated and collects networking packets of data and tests their quality for any connection using the predetermined established new attacks. This software is most commonly used to stop known attacks by the machine. This is a statistical classification that determines that a specific class and would have a specific network occurrence. These have greater quality and speed than some other classifiers. Z is a package that is provided, G is an assumption, Z is given to class D. The main aim is to estimate the possibility {QUOTE Q *(G / Z)*} , the assumption is to get the package Z, Q(Z) is the starting possibility. The starting possibility{QUOTE *Q (G / Z)*} of assumption G, on the package Z is shown in Equation (1) and it is illustrated in figure 4

$$\{\text{QUOTE } Q\,(G/Z) \quad \frac{Q\,(G/Z)\ x\ Q(G)}{Q(Z)} \quad \}$$

(1)

For constructing the tree structure, Statistical classifier algorithm attempts to settle in over-fitting problem and selects the parameter as the scatter parameter as per the abundance dependent performance gain.

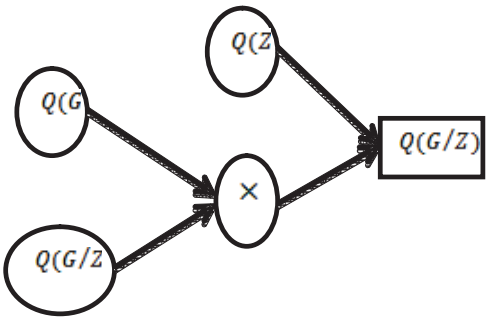


Figure4. The initial possibility and the assumption rate

The initial step in Statistical classifier algorithm describes { QUOTE *IF (E)* }, indicates the uncertainty from the learning given data E, and the likelihood that such specific example from E is a {QUOTE D_j }. The definition for {QUOTE *IF (E)*} is shown in Equation (2)

$$\{\text{QUOTE } IF\,(E)\ \}\ IF(E) = -\sum_{i=1}^{l}[\frac{|E_i|}{|E|}\log_2[\frac{|E_i|}{|E|}]]$$

(2)

The term profit (Z) is a function of the quantities obtained by dividing E by Z (enable to handle the sign layout, specified as parameters within our system), per the element Z. The profit (Z) is shown in Equation (3)

$$\{\text{QUOTE } \ profit(Z) = IF(E) - \sum_{i=1}^{l}[\frac{|E_i|}{|E|}IF(E)]$$

(3)

Here { QUOTE E_i } refers to verify information couple of iterations. The profit analysis is shown in Equation (4)

$$\{\text{QUOTE } \ profit_{an}(E) = \frac{IF(E)}{-\sum_{i=1}^{l}[\frac{|E_i|}{|E|}\log_2[\frac{|E_i|}{|E|}]]}$$

(4)

As the controversial parameter in the decisional chain, the average accuracy benefit rate is chosen. The set of data is then split into multiple subgroups depending on the feature value. Additionally, a different feature is chosen and that each section is subdivided. The separating process repeats till every sub-set of the information is from the same category or the win proportions are just the same. The tree structure for Statistical classifier algorithm is shown in figure5.

Figure5.The tree structure for different class

Based on the mathematical equation, Statistical classifier algorithm based signing detection method (SA-SDM) is used for the reduction of the DDoS attacks risk. Statistical classifier algorithm reduces the attacks occurring in the cloud and network services

IV. RESULTS AND DISCUSSION

In this section, Statistical classifier algorithm based signing detection method presents the essential concepts, principles and terms necessary for experimental study. Consequently, there is clarification on the main elements of the proposed method. Any DDoS attack can have an effect on the public clouds. The proposed method consists of the intended Physical Machines linked via the internal Internet Protocol adapter to a network. The adapter is linked to the Internet via the external Network access point. DDoS flood attacks are the type of threat that this test intends to measure. The best classification accuracy for DDoS attacks by SA-SDM is shown in table1.

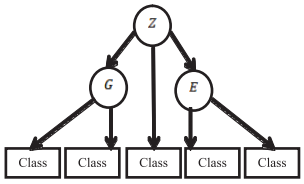


Figure5.The tree structure for different class

Table1. The classification accuracy for DDoS attacks by SA-SDM

Total Number of Iterations	Naïve Bayesian	C4.5	K-means	SA-SDM
50	79.99	64.67	74.66	87.09
100	55.68	42.32	90.12	91.08
150	47.21	79.24	88.88	89.02
200	90.90	85.12	62.45	88.35
250	41.57	78.99	52.11	98.95

The proposed method uses a data type script file for the production of ordinary internet traffic that uses the developed model for the separation of threat and ordinary data. The classification accuracy for DDoS attacks by SA-SDM is shown figure 6.

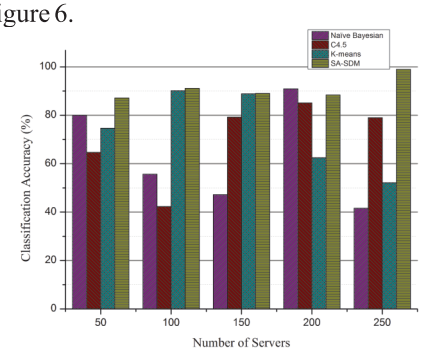


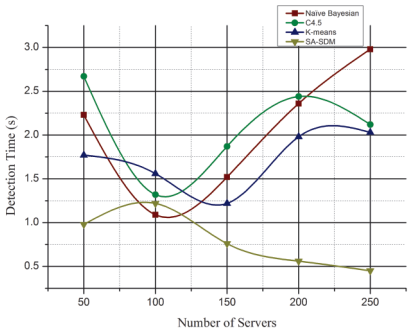
Figure 6. The classification accuracy for DDoS attacks by SA-SDM

The detection time for DDoS attacks by SA-SDM is shown in table2. The right identification and measurement of the attack time, in 0.45s duration. The proposed method when compared with Naïve Bayesian, C4.5, K-means, the detection time taken by SA-SDM gets best result.

Table2. The detection time taken by SA-SDM

Total Number of Iterations	Naïve Bayesian	C4.5	K-means	SA-SDM
50	2.23	2.67	1.77	0.98
100	1.09	1.32	1.56	1.22
150	1.52	1.87	1.22	0.76
200	2.36	2.44	1.98	0.56
250	2.98	2.12	2.03	0.45

Figure7. The detection time taken by SA-SDM



In fact, the greater the detection accuracy rate for this program, with the rise in the period of DDoS attacks. This service feature check outcome demonstrates that it can satisfy everyday needs. The detection time taken by SA-SDM is shown in figure7.

Dependent on prediction (PR) accuracy (QUOTE *RE*)} , k-value is measured. The following is the estimated value and it is shown in Equation (5), (6), (7)

$$\{ \text{QUOTE } prediction = \frac{RP}{RP+WP} \} \quad (5)$$

$$\{ \text{QUOTE } RE \quad RE = \frac{RP}{RP+WN} \} \quad (6)$$

$$\{ \text{QUOTE } K - value = \frac{2*accuracy*R_e}{accuracy+R_e} \} \quad (7)$$

Here RP represents the real positive values, WP refers the wrong positive values, WN, refers the wrong negative values, RE refers the prediction value. Accuracy shall be specified as a division of items properly predicted positive from all factors correctly recognized by the formula, while reminder shall be defined as the percentage of items correctly recognized from all positive aspects. The accuracy rate by SA-SDM is shown in Figure8

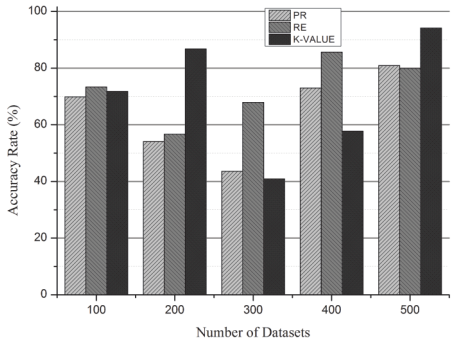


Figure 8. The accuracy rate by SA-SDM

PR is the prediction; RE is the accuracy rate, k-value achieved by SA-SDM is shown in figure9. The study of attacks on DDoS finds the good sensitivity and output performance of the device that can be found and overall performance is shown in experimental analysis.

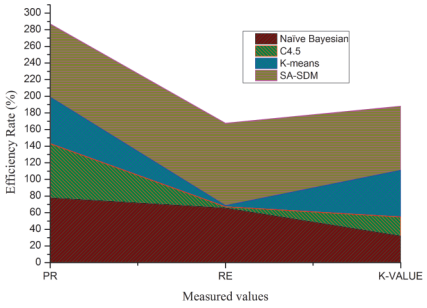


Figure9.The overall measured values achieved by DA-SDM

Based on system framework, Statistical classifier algorithm based signing detection methods (SA-SDM) are used for the reduction of the DDoS attacks risk.

V. CONCLUSION

This research provides information regarding, Statistical classifier algorithm based signing detection methods (SA-SDM) for the reduction of the DDoS attacks risk. Statistical classifier algorithm reduces the attacks occurring in the cloud and network services. This, along with signing detection methods, provides a technique to find signing attacks automatically and effectively for DDoS replay attack. A benchmark review is provided for various master learning methods and algorithms. The proposed method SA-SDM is used to detect DDoS attacks by using an algorithm Statistical classifier provides more precise results than other machine learning techniques.

REFERENCE

1. Atzori L, Iera A, Morabito G. From" smart objects" to" social objects": The next evolutionary step of the internet of things. IEEE Communications Magazine. 2014 Jan 16;52(1):97-105.

2. Misra SC, Mondal A. Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. Mathematical and Computer Modelling. 2011 Feb 1;53(3-4):504-21.

3. Voorsluys W, Broberg J, Buyya R. Introduction to cloud computing. Cloud computing: Principles and paradigms. 2011 Feb 28:1-44.

4. Ouaddah A, Mousannif H, Abou Elkalam A, Ouahman AA. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks. 2017 Jan 15;112:237-62.

5. Sultan N. Cloud computing for education: A new dawn?. International Journal of Information Management. 2010 Apr 1;30(2):109-16.

6. Fan Z. A distributed demand response algorithm and its application to PHEV charging in smart grids. IEEE Transactions on Smart Grid. 2012 Mar 13;3(3):1280-90.

7. Abolfazli S, Sanaei Z, Ahmed E, Gani A, Buyya R. Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials. 2013 Jul 19;16(1):337-68.

8. Alomari E, Manickam S, Gupta BB, Karuppayah S, Alfaris R. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403. 2012 Aug 2.

9. Brettel M, Friederichsen N, Keller M, Rosenberg M. How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 Perspective. International journal of mechanical, industrial science and engineering. 2014 Jan;8(1):37-44.

10. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials. 2015 Oct 5;18(1):602-22.

11. Tripathi S, Gupta B, Almomani A, Mishra A, Veluru S. Hadoop based defense solution to handle distributed denial of service (ddos) attacks.

12. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE communications surveys & tutorials. 2015 Oct 5;18(1):602-22.

13. Choo KK. The cyber threat landscape: Challenges and future research directions. Computers & security. 2011 Nov 1;30(8):719-31.

14. Alkasassbeh M, Al-Naymat G, Hassanat A, Almseidin M. Detecting distributed denial of service attacks using data mining techniques. International Journal of Advanced Computer Science and Applications. 2016 Jan 1;7(1):436-45.

15. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of Cloud computing. The journal of supercomputing. 2013 Feb 1;63(2):561-92.

16. Iyengar NC, Banerjee A, Ganapathy G. A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment.

International journal of communication networks and Information security. 2014 Dec 1;6(3):233.

17. Wang B, Zheng Y, Lou W, Hou YT. DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks. 2015 Apr 22;81:308-19.

18. Rawashdeh A, Alkasassbeh M, Al-Hawawreh M. An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology. 2018;57(4):312-24.

19. Bhuyan MH, Bhattacharyya DK, Kalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognition Letters. 2015 Jan 1;51:1-7.

20. Kato K, Klyuev V. An intelligent DDoS attack detection system using packet analysis and Support Vector Machine. Int. J. Intell. Comput. Res. IJICR. 2014 Sep;14(5):3.

21. Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE transactions on information forensics and security. 2011 Jan 20;6(2):426-37.

22. Leu FY, Lin IL. A dos/ddos attack detection system using chi-square statistic approach. Jour. of Systemics, Cybernetics and Informatics. 2010;8(2):41-51.

23. Jia B, Huang X, Liu R, Ma Y. A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning. Journal of Electrical and Computer Engineering. 2017 Jan 1;2017.

24. David J, Thomas C. DDoS attack detection using fast entropy approach on flow-based network traffic. Procedia Computer Science. 2015 Jan 1;50(4):30-6.

25. Choi J, Choi C, Ko B, Choi D, Kim P. Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment. J. Internet Serv. Inf. Secur.. 2013 Nov;3(3/4):28-37.