



An enhanced agent protection model for securing cloud computing against DDoS attack

Husam Saleh Mahmood¹, Shawkat Kamal Guirguis², Wagdy Gomaa El-sayed¹ and Shaimaa Ali El-sayed el-morsy¹

¹Faculty of Science, Alexandria University, Alexandria University, Egypt

²Department of Information Technology, Institute of Graduate Studies & Research, Alexandria University, Egypt.

2628

ABSTRACT

Nowadays, online availability of the internet resources has proven efficient means of information sharing. Cloud computing environment provides a managed computer system resources to the internet users and companies with options of processing, storage, management and access to data and information within a certain server. Several types of attack can target cloud environment, among these types of attack DDoS attack considered as the most common and dangers type. In this work, a protection system for securing cloud computing environment against DDoS attack has been proposed. The system is designed based on the most common and effective machine learning techniques which is SVM that used for traffics detection and classification. Also, an improved software agent is used as a complemented to the SVM, for anomaly traffics control. Testing dataset is required for test and evaluate the performance of the proposed system, therefor CIDDS dataset has been used. However, according to the obtained results, it is observed that the proposed system achieved the highest results with accuracy of 99.6% in anomaly traffics classification and control during the comparison with the related work.

DOI Number: 10.14704/NQ.2022.20.12.NQ77245

NeuroQuantology2022;20(12): 2628-2641

1. INTRODUCTION

Cloud computing is defined as the processing, storage, management and access to data and information within a certain server. The infrastructure and servers are provided available "on need" basis by the use of cloud computing[1]. Cloud computing also includes network-enabled, scalable, assured Quality of Service, low-cost computing infrastructure, and simple accessibility services. Cloud computing is becoming a buzz word in the IT sector, with many users migrating their apps and data to a distant cloud [2]. Users have more flexibility in how they access data and apps. Despite its advantages, cloud computing is now in its development and faces several hurdles in terms of security, integrity, cost, availability, and performance. The biggest challenge with cloud computing is cybersecurity, because the thought of saving private data or running software on another's hard disc might be unsettling to some users[3]. Greater specifically, the increased usage of cloud computing by businesses provides more options for hackers to gain unauthorized access to virtual environments[4]. As a result, engineers have created a revolutionary virtualized security method to combat the threats.

Additionally, Cross-Site Scripting, SQL Injection, and Distributed Denial of Service attacks are also common in Cloud computing system. The most dangerous sort of cyberattack that might strike cloud computing is a distributed denial of service (DDoS) attack. DDoS assaults are a serious risk to cloud security's reliability. DDoS assaults have more potential in cloud computing, which includes millions of subscribers

exchanging infrastructure than they do in sole tenancy design [5]. DDoS cyberattacks may be carried out in two methods via the Internet. The first approach entails an attacker delivering malicious files to the target in order to confuse any programme or protocol operating on it (vulnerability attack)[6, 7].

Financial fraud including unlawful cash transactions is one of the grounds for the attack. Collecting a commission from a viewed advertisement display is a common example of this type of financial scam [5]. Other attacks, including political attacks, are carried out in benefit of a nation, whereas personal attacks are carried out for personal reasons [7, 8]. In other words, cyberattacks happen for a variety of motives and at various degrees. Furthermore, the most prevalent sort of attack is a Distributed Denial of Service (DDoS) attack, which is an attack on a system that fills it with so many additional requests that normal traffic is either delayed or entirely disrupted. SQL Injection is also regarded as a security flaw that occurs in the databases of a cloud servers. Cross-Site Scripting is when a malicious script is executed by a user's Web browser [8]. Password cracking is the technique of retrieving confidential passwords from stored data in or communicated by a computer system, usually by confirming password guesses repeatedly [9].

The Distributed Denial of Service (DDoS) is among the most dreaded cyberattacks, and it poses various security issues in today's networks. They are able to interrupt system reliability by depleting a large number of resources by causing traffic congestion. However,



DDoS cyberattacks, which are well-planned strikes with a high degree of intensity that may disrupt the highest level of information infrastructure [10, 11], are one of the biggest risks that the modern electronic society faces. The accessibility of many hacking tools makes it simple to carry out such attacks. However, in order to employ the existing hacking tools, the attacker must have the necessary skills. In a perfect world, one must be able to distinguish among abnormal and typical traffic.

SVM and Software agent have been identified to be utilized to supplement filters in the literature; it is one of the methods that the network may continue to function even while under assault [10]. An agent is any type of hardware or software which is utilized independently for detection and sensitive to external changes using properties such as adaptively, mobility, and learning ability [11]. The agent is introduced to the network in order to improve the network's ability to continue working even when it is attacked, as well as to provide flexibility and agility in solutions targeted at resolving the network's current and future challenges [12].

This study focuses on DDoS cyberattacks, which are a big danger to the cloud computing ecosystem. The goal of this study is to enhance the security mechanism against DDoS assaults on cloud computing environments. Following that, this study suggests using a hybrid of SVM for anomaly traffics classification and software agent for traffics control. Therefore, it is designed to improve the protection model against DDoS attack traffics aimed at cloud computing environments.

This work is segmented into seven sections, the background of the work is presented in section 1. In section 2, the most related work has been discussed. Whereas, the research methods which have been used in this study is illustrated in section 3. The proposed system architecture is presented under section 4. Furthermore, the implementation and results of the proposed system is illustrated and displayed in section 5. Also, the discussion of the work is presented under section six. Lastly, in the 7 section, the conclusion of the work is presented.

2. RELATED WORK

Cloud computing is a framework that allows end users to connect to sophisticated applications and services through the Internet. It is critical to deliver secure and dependable services in the cloud computing environment. One of the security concerns in this context is how to decrease the impact of a denial of service (DoS) or disseminated denial-of-service (DDoS) attack [9, 13].

Ojugo et al. [14], in this study an intelligent systems based on machine learning has

been proposed. The effective machine learning technique which is neural network has been employed for anomaly traffics classification and attack detection. In addition, the deep learning technology is utilized to discriminate between benign data exchange and harmful data traffic attacks. Furthermore, the results show that using a neural network to efficiently discern between acceptable and non-approved data packets on a data traffic is a success. However, according to the obtained results it observed that the proposed system achieved a good result with accuracy of 96%.

Chauhan and Heydari [13] they design an intrusion detection system that has the ability to defines against DDoS attack in Generative Adversarial Networks (GNAs) environment. The proposed model is adopting with the GAN to generate adversarial DDoS attacks that can change the attack behavior and can be undetected. However, the results indicate that by continuous changing of attack behavior, defensive systems that use incremental learning will still be vulnerable to new attacks. The proposed system achieved a good result during the comparison with the related work with accuracy of 94.3%.

Saad et al. [15] proposed an intelligent flooding-attack detection system using back-propagation neural network. The proposed system has the ability to defines against DDOS attack in IPv6 networks. The efficiency of the designed system is proved by using real datasets gotten from an NAv6 laboratory. The dataset traffic is based on a test-bed environment created on the basis of certain parameters used as inputs to generate a new data-set. The results prove that the proposed framework is capable of detecting ICMPv6 DDoS flood attacks with a detection accuracy of 98.3%.

Wang et al. [16] examine the security effect, namely the influence on DDoS attack define mechanism, in an enterprise network in which both technology are used, and conclude that SDN technology may really assist organisations fight against DDoS assaults provided the defined structure is correctly constructed. To that aim, they offer a DDoS attack mitigation architecture that combines take several forms network monitoring to identify attacks with a customizable control framework to allow for quick and precise attack response. They offer a visual model-based detection and prevention system for dealing with dataset shifting problem to cope with the new architecture. They offer a visual model-based detection and prevention system for dealing with dataset shifting problem to cope with the new architecture. The simulation findings demonstrate that the structure can efficiently and effectively meet the security concerns posed by new network paradigm, and that our attack detection system can identify and report a variety of attacks employing real-world network data.



Wani et al. [17] used Tor Hammer as assaulting tool and built a fresh dataset with Intrusion Detection System on their own cloud environment. There are 9 features and 4 classes in the dataset. The data set was subjected to machine learning algorithms such as Support Vector Machine, Nave Bayes, and Random Forest. Because of its strong performance, the SVM model may be utilised for intrusion detection. Wani et al. (2019) used various machine learning techniques for classification, which includes Support Vector Machine, Random Forest, and Nave Bayes, with the precision of 99.7%, 97.6%, and 98.0 percent for Support Vector Machine, Nave Bayes, Random Forest, respectively.

3. RESEARCH METHOD

The research methods and material which have been used in this work are illustrated in this section:

3.1. Datasets Description

Benchmark datasets are required for testing, evaluating and validating assumptions for the researcher's methodology. However, the hardest issue for working on DDoS attacks is to find suitable datasets. It is a considerable challenge since the availability of such datasets is very rare. Subsequently, there are several types of security datasets such as CIDDS, DARPA, and KDD available to be utilized [18, 19]. These datasets can be utilized in the detection of several types of attacks as well as for systems assessment. However, existing datasets also post additional limitation as most of them are outdated. Due to numerous new types of attacks and security technology for detecting DDoS attack flooding traffics-based network anomalies, there is a need to find a new and suitable dataset to test and evaluate the proposed model. Nevertheless, CIDDS 2017 is a conception used for the creation of datasets that will be used for evaluation of anomaly-based network intrusion detection systems [19].

Therefore, the primary objective of using CIDDS 2017 in this study is that it is current and customizable. The additional program of C# programming language is used in a virtual environment to regenerate customized datasets that can be used in this work. Basically, the dataset was chosen because; it is recent, online available and free, it can simulate real-time processing because it has the duration features, it has the attributes of several types of Flooding attack.

3.2. Support Vector Machine (SVM)

Linear models, such as SVM, are used for regression analysis and classification. Several practical problems can be solved with it, including linear and non-linear problems. SVM is based on the idea that data is grouped into classes

by creating a line or hyperplane. In order to use Linear SVM, the data must be perfectly linearly separable, meaning each point can be classified into 2 classes using a single straight line [2]. However, if the data cannot be segmented linearly, then we can use Non-Linear SVM. In other words, when 2D data points cannot be classified easily into 2 classes, we resort to other advanced approaches like kernel trick classification. Real-world applications rarely involve linearly separable data, so we can use kernel tricks to solve them, as in IP request datasets and network traffic datasets [20, 21]. Using Non-Linear SVM, we can classify and separate the IP into different groups.

3.3. Software Agent

Agents are a mix of equipment or software elements that are responsive to their clients' needs, independently of each other. Among its many useful qualities are learning, adaptability, connectivity, reactivity, autonomy and proactivity. Adaptive agents are applicable to a variety of domains, including portable processing, data recovery and processing, smart communication, media communication, and e-commerce [19]. Agents are directed in different ways to serve particular clients or to perform specific tasks in a multi-agent framework. Self-governance, adaptability to failures, dynamic setup, sovereign decision making, studiedness, and scalability were the factors that led to the use of agent technology in this project [2, 22]. The agent may attempt from time to time to adapt to its new or dynamic condition or to handle new or changing objectives. Using it as a complement to SVM for anomalous traffic filtering, it controls two filters.

3.4. Evaluation Methods

The evaluation of the proposed model uses the accuracy which is the most popular measurement for evaluating the performance of the proposed systems related to protection systems [2, 5, 23]. Moreover, these measurements are obtained from the parts of the matrix elements. The elements that make up the chaos frame include true positive (TP), true negative (TN), false positive (FP), and false negative (FN). In general, TN is characterized by the number of events that are usually called effective. TP is representing the number of samples accurately referred to as attacks. CE is a level of sampling of attacks incorrectly organized as routine events. In essence, the UN is the scene of common events falsely classified as aggression. The accuracy is characterized by the fact that the proportion of all events is accurately classified (TP, TN) (TP, TN, FP and FN) in all cases. The ratio between TP and total TP and CE is exact positive predictive value. Accessibility is the ratio of TP to the sum of TP and FN. In this work, an accuracy calculation is given in Equation 3.12.



4. THE PROPOSED SYSTEM

There are many methods proposed to defend against DDoS attack as discussed in the literature but the performance is still not good enough. This work proposes the flooding attack Protection model to protect cloud computing servers against flooding attacks. The proposed model monitors and controls anomaly traffics, it consists of three stages, which are Anomaly Traffic Detection Stage (ATDS), Anomaly Traffics Classification Stage (DATCS), Anomaly Traffic Control Stage (ATCS) as described in the following subsections. However, the architecture of the proposed system is illustrated in Fig. 1.

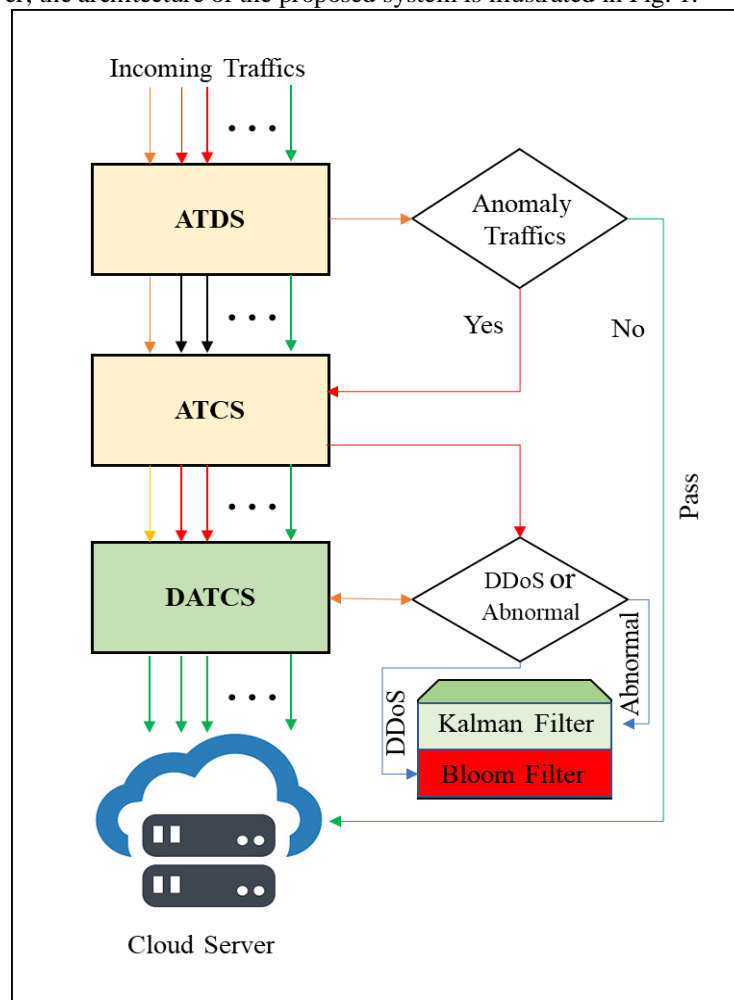


Figure1. The architecture of the proposed system

4.1. Anomaly Traffic Detection Stage (ATDS)

The main module in the APFA model is the Abnormal Traffic Detection Stage (ATDS). The ATDS is the Anomaly Traffic Detection Stage (ATDS), it can be a product device or application or device which could filter frame exercises or network traffic to detect strategic harms or harmful exercises and report to the management station. The cycle aids to differentiate intrusion because the potential of the intruder’s scheme is unique compared to the actual user’s behaviour. Its use is largely close to other security measures that activate countermeasures[19].

This stage was designed to filter analyses and gradually distinguish in real time an abnormal traffic. The presence of this stage is mainly in the frontend sensors. It dispels the fundamental about how standard traffic behaviour relates to the use of a typical framework, or the main aberration from common behaviour may be exciting. Therefore, the objective is detection any unexpected alteration that is happening. The fundamental emphasis towards the module is when the modelling is accomplished, the output of the model can be related to the typical behaviour and a strange understanding is gained by distinguishing between the



observed behaviour and output of the model [16, 24]. The signature is calculated assignal that shows where it ended up as an identifiable component of DDoS attacks, and then helps separate whether this could be DDoS traffic or unusual trading. There are many fruitful applications based on such ideas in online traffic investigation.

The main objective of this module is identifying unexpected changes in GET requests delivered to the front-end sensor, also known as anomaly detection. If there are no abnormalities observed, this module does nothing. If aberrant data is found in traffic coming, a "attention" signal is delivered to the following phase, the Anomaly Traffics Classification Stage (ATCS), which does more traffic analysis. Before transmitting an attention signal, many procedures must be completed, as shown below.

The first step is to examine the incoming traffic. This may be accomplished in a variety of ways; however, the suggested method uses an Auto Regression (AR) model to predict traffic intensity [15]. Previous results have an influence on future results in regression; hence, the AR model utilizes previously identified traffic to help predict traffic intensity changes.

The DNS GET traffic stream is initially monitored. The traffic intensity is observed in fixed intervals of time periods and forms a time-series $\{y_{-1}, y_{-2}, \dots, y_t\}$. In this research work traffic intensity is calculated in this thesis "by the total number of packages received in a time interval"[16]. The Shannon entropy is used to forecast the traffic intensity based on previous data [13]. If there are significant changes, it might be a network application layer DDoS assault. The AR model that predicts the current traffic intensity can be calculated by Equation 3.6.

(2)

The variable y_t represents the predicted value of the variable x_t , which is the observation value at time t . The variable a_t^k is a "stationary model parameter," meaning it does not change as time passes, and the observation error is e_t [16, 25].

Second, the difference here between measurement x_t and the forecast y_t at a given time t yields the residual or model error x_t , as shown in Equation 3.7. A standard deviation σ_d^2 may be derived from that specific residual at time t , as shown in Equation 3.8.

(3)

Thirdly the standard deviation σ_d^2 :

(4)

Now, a threshold was seen in Equation 3.9 and Equation 3.10, can be generated by determining either traffic is abnormal or not. If d_t is greater than $k\sigma_d^2$ abnormal traffic is perceived and an consideration signal is delivered to DADS for further analyses. In the opposite case when abnormal traffic is not detected, the ATDS module transmit a signal to dismiss to DADS module which deactivates automatically. The sensitivity of the threshold is adjusted by the constant k , which is not fixed to a specific value.

(5)

and

(6)

4.2. Anomaly Traffics Classification Stage (ATCS)

The Anomaly Traffics Classification Stage (ATCS) is the second unit of the proposed model. In this stage, the most effective classification method based on machine learning which is Support Vector Machine (SVM) has been employed. The suitable machine learning method is chosen to build the model for detection based on the succession of functions value samples, the modeling is used to classify the unlabeled characteristic value samples. The classification learning approach used in this work is basis on the support vector machine (SVM) algorithm [14, 15] SVM is a statistical learning theory-based learning approach. Without large training data, it may produce decent classification results. It linearizes the nonlinearly separated sample set by mapping it to a high-dimensional or even infinite-dimensional feature set and then finding the best classification surface in that space. The two-dimensional scenario may explain the core



principle of SVM, which is concluded linearly separable optimum classification hyper plane. SVM's kernel function successfully addresses the dimensionality catastrophe produced by high-dimensional mappings and improves the capacity to analyse high-dimensional small sample data. SVM accomplishes the sample categorization by looking for the sample with the biggest classification interval. The equation can be used to express the best classification line 7;

(7)

Where, b is the scalar and w is the weight vector and likewise, the separation hyper plane satisfies the below points

(8)

We may change the weight so that the hyper plane's edge side can be stated as

$$H1 : w * x + b \geq 1 \text{ for } y_i = 1 \quad (9)$$

and

$$H1 : w * x + b \leq 1 \text{ for } y_i = -1 \quad (10)$$

This indicates that vector that fall on or above $H1$ are in class +1, whereas vectors that fall on or below $H2$ are in class 1.

The equal sign is established if any of the training tuples that fall on $H1$ and $H2$ are support vectors. We may deduce from the above that the greatest edge is $2/|w|$. Calculating the minimal value of $|w|$ is similar to finding the largest value of $2/|w|$. The method by which the SVM identifies the optimal hyperplane in n -dimensional space is comparable to solving the restricted optimization problem; the following formula is followed:

(11)

where $C > 0$ is the penalty parameter, which shows attention degree to the outliers.

We utilize the SVM method features, gather switch data and extracting the characteristics to train, find the ideal hyperplane amid both the normal data and DDoS cyberattack information, and to receive the classification results using our proposed model test data.

Moreover, in order to differentiate the DDoS traffic from normal traffic for each IP address, the calculations for entropy values of the incoming traffics in different period of time have been done. The purpose of these calculations is to provide a description of the distribution of incoming sources and the target URLs. Next is to determine the source of each IP address that sends anomaly traffic in the DADS module. Then, it will send to the last stage in the proposed system which is DDoS Attack Traffic Control Stage (DATCS) for further analyses.

4.3. DDoS Attack Traffic Control Stage (DATCS)

This work contributes the Adaptive Traffic Control (TCM) Stage. The TCM is agent in which it is deployed to perform the adaptively decisions. The autonomous capabilities of the agents are supported by facilitating the selection of tasks based on states of beliefs. These beliefs aid the agent in making judgments about the activities necessary to achieve the tasks. Observing the incoming traffic behavior and managing the traffic flow are two of the jobs.

The agent controls the traffics by employed two filters which are Kalman filter and bloom filter. The Kalman filter contains a handful of numerical equations that allow condition of processing with high-performance computer equipment to be assessed with the ultimate goal of limiting the average error. The capabilities of the filter can be viewed from several perspectives: it evaluates the past as it does today, regardless of whether the exact type is unclear in the frame presented. In the proposed model, the Kalman Strait is under the control of the agent. The specialist refers commands to the Kalman Filter to start or turn them off after measuring predefined limits and nearby traffic, after imperfect irregular flood meters. Whereas Bloom filter can be considered the most spatially probable form of information. Furthermore, to determine if an element is a member of set it can also be employed. For example, a question might come back as "not in a set" or "maybe in a set". Modules is added to the equipment that has not yet been switched off. At the end of



the day, the probability of false positives increases, and components quantity added to the equipment increment [13]. In the proposed model, the specialist controls the pathogen. The expert directs comments to the Bloom filter to start or stop it, which depends on predefined limits and the amount of incoming traffic when DDoS attack traffics have been recognized, as previously explained.

The TCM agent has a reactive adaption in which it performs adaptation to the traffic through implementing two functions which are anomaly traffic handling, and anomaly traffic diagnosis. The values of two pre-existing variables, traffic attack behaviour and normal traffic intensity, are used to execute these functions. Information regarding traffics is included in the belief elements in both the normal and abnormal cases. Desires, often known as objectives, are a reflection of what the agents hope to accomplish. Desires or objectives can be expressly created or generated during runtime by the agent. However, at this point, the goals are established by the related tasks, which will be discussed later. Finally, intentions are linked to plans, which are organized sequences of activities aimed at accomplishing the goals if there is a way to do so.

In addition, the agent's objectives are distinct from the plans. There may be numerous strategies in place for reaching a result, hence if one failed, the agent uses the reasoning cycle to evaluate alternative options. When numerous plans to attain a goal exist, there is a selection function that allows the most suitable and applicable plan to be chosen instead of the random selection strategy.

When the DATCS receives anomalous traffic with IP address from source ATCS, the DATCS controls the incoming traffic using the two specified parameters. When the DATCS receives anomalous traffic with the source IP address from the ATCS, the DATCS controls the incoming traffic using the two specified parameters. In the agent first stage, the very first function compares the current traffic intensity to the regular traffic intensity; if the traffic conditions intensity is greater than the normal normal traffic traffic intensity, an attack traffic state exists; if the traffic conditions intensity is below b_1 , a normal traffic state exists, and traffic is routed to the cloud server.

After determining that incoming traffic is being attacked at the second stage of the agent, the second function will diagnose the type of traffic based on the traffic's behaviour, if it is DDoS or abnormal traffics. In case of the DDoS, the traffic is sent to bloom filter for permanent block. In case of the abnormal traffics, the traffic is sent to Kalman filter to temporary block some of it.

5. IMPLEMENTATION AND RESULTS

- Software: C#, accessible for 2013 visual studio, Windows 10, was used in this study. In comparison, various libraries, groups, and functions can be found in C#, which implies it is chosen.
- Hardware: The simulation is run on a single laptop with an Intel (R) Core (TM) i7-5500U CPU running at 2.40GHz and 16 GB of RAM.

5.1. Implementation Modelling

The purpose of this study is to strengthen the defence mechanisms that target DDoS attacks. The protection model is critical to be able to identify, categorise and track the attack traffic. In the following subsection, the dataset setting. The CIDDS 2017 dataset attributes are evaluated to better understand the stimulation level [19]. A large number of DNS requests, including normal DNS requests and irregular DNS requests, are generated using the CIDDS 2017 dataset. It is then divided into three different groups of traffics (normal, anomaly, and attack).

In addition, the total transactions were split into two parts, with the first portion being used for system training 60% of the dataset, and the second segment representing 40% of the dataset for testing. Furthermore, the CIDDS 2017 dataset is separated into four weeks. The Week 1, Week 2, and Week 3 datasets are used for training purposes and contain 39,539 IP addresses which send 567,718 requests. The first week consists of 12609 IP addresses sending 207,035 requests, and the second week consists of 9556 IP addresses sending 159,373 requests, and the third week consists of 8503 IP addresses sending 153,026 requests. Whereas the fourth-week dataset used for analysis comprises 8871 IP addresses and 186,004 requests have been sent.

In addition, as a consequence of the benchmark analysis, the validation stage incorporated the categories of normal, anomaly and attack traffic, which can only cope with two modes of traffic that are normal traffic and attack traffic. There are many ways to protect against DDoS attacks and each technique uses specific parameters. Even so, the study used several criteria and variables. The latter half of this chapter explores these two additional requirements.

The proposed model is designed to protect the DDoS attack at the application layer level. The overall simulation processing model, starting with the Abnormal Traffics Detection step (ATDS) (Step 1 and 2) which obtained the dataset to set the threshold by monitoring and evaluating the incoming traffic imported from the data set, as shown in the bellow Fig. 2. In addition, according to the ATDS analysis, the threshold is obtained. Whereas, in the case of incoming traffic, less than the limit may have elapsed. Conversely, if the incoming traffic is higher than the threshold, the traffic would submit an important signal to the ATCS or



further analysis. However, the ATCS will start tracking the source of each IP address that sends anomalies to the traffic (Step 3). The source of these IP addresses will then be specified by the ATCS and forwarded to the DATCS for further analysis (4). In comparison, these elements allow it possible to differentiate what an agent wants from how the target is reached.

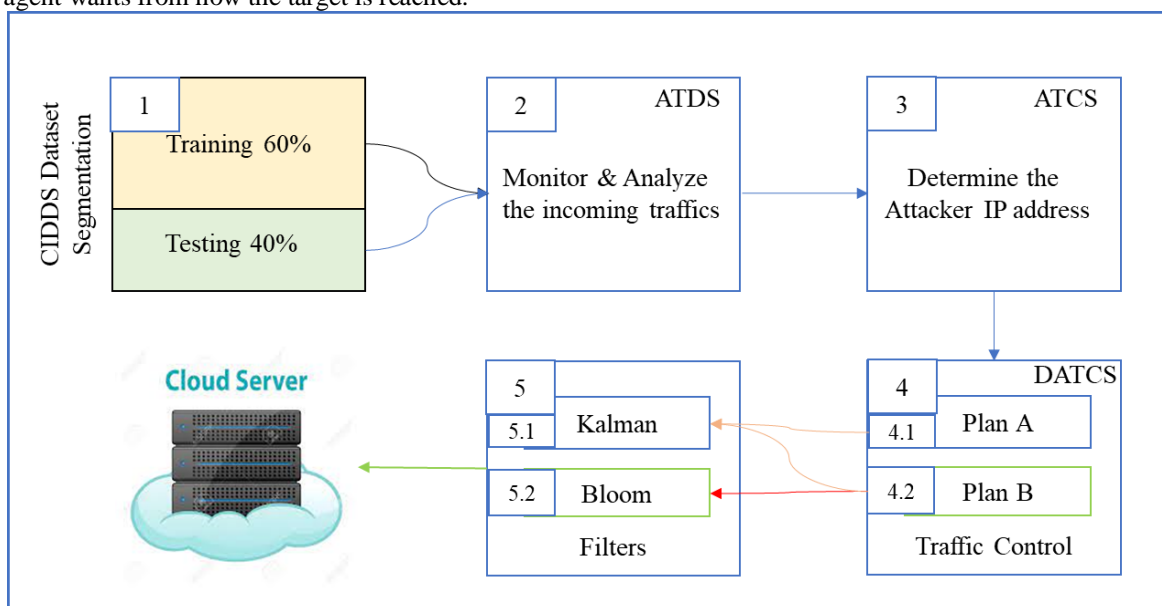


Figure 2. Steps of the Simulation Design

As a result, there are two plans to identify and control traffic. First, plan A will be passed in the case of incoming traffic below the threshold (Step 4.1). On the other hand, if the incoming traffic exceeds the threshold, the next plan will be forwarded for further analysis. Second, in the case of abnormal traffic following Plan B (Step 4.2), which is used to distinguish and separate attack traffic, attack traffic is classified as DDoS and abnormal traffic following traffic behaviour. However, the anomaly traffic sends the temporary block to the Kalman filter (step 5.1) and the DDoS traffic sends for permanent block to the bloom filter (Step 5.2). Note that the system is running twice during the implementation phase, one for training and the other for testing. At the training stage, the dataset of the first three weeks 1, 2 and 3 were used to set the parameters and to obtain the conditions. Whereas the dataset for Week 4 was used to test and evaluate the system at the test stage.

5.2. Experiments Results

The models and measurements used to determine the effectiveness of the proposed model are described in this section. The studies examine the impact of the Distributed Denial of Service and Forced Causality attacks to evaluate the proposed model performance. The proposed model is evaluated and compared to tasks in the dataset and the results are then tested against this dataset directly. The proposed technology is compared with the related work of Ojugo Arnold [14], Chauhan and Heydari, [13] and Saad et al [15].

In addition to Segment 4 of the study, the robot is also being fitted with a new brain and operating out of a new location. In addition, 60 percent of the data for the study's dataset is from the sampled IP addresses. Finally, the robot, which has been programmed by the study, has made a combined total of over a hundred thousand requests, all geared toward keeping the database growing. At the stage when the specifications are available, the requirements of the device are obtained. On the other side, 40 percent of CIDDS dataset for the fourth week was used to test this model. The fourth-week dataset comprises a totally of 8871IP addresses and 186, 004 requests, as seen in Fig. 3 and it without action from the system. Also, the traffics in the fourth week was divided into four days starting on day 1, with a demand of 48133 and ending with the 36397 requests.



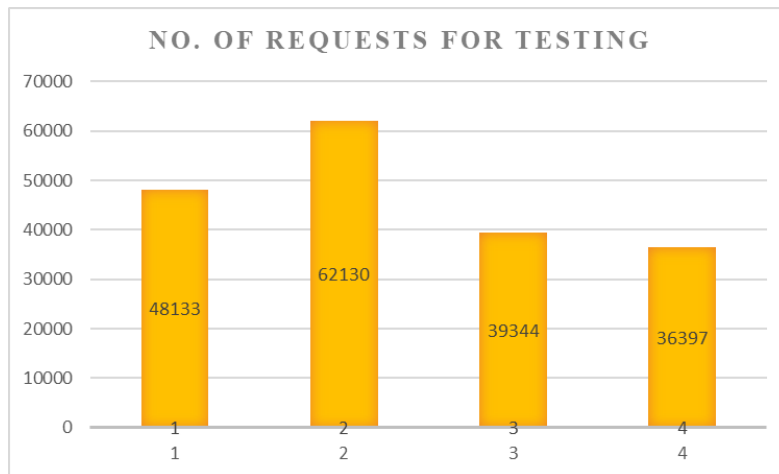


Figure 3. Incoming Requests for testing dataset

Moreover, as the discussion which has been done in the above sections, the threshold is determined at the Anomaly traffic detection stage (ATDS) by analyzing the behavior of the incoming traffics at different period and days. The main goal of this module is to identify unexpected changes in GET requests delivered to the front-end sensor, also known as anomaly detection. If there are no abnormalities observed, this module does nothing. If from incoming traffics abnormal information is noticed, an "attention" signal is sent to the next phase Anomaly Traffics Classification Stage (ATCS), which gives further analyses for the traffics.

Subsequently, when the threshold is determined the ATCS will start classifying the traffics by using the SVM kernel. Then, as seen on the right side of Fig. 4, the mapped instances in the training set may be linearly separated in the new space. The amount of traffic which have been received for the fourth week is 186, 004 requests which generated from 8871IP addresses. The traffic was classified by the ATCS, and the attack traffic was blocked after the system was detected. To classify the incoming anomaly traffic into DDoS and abnormal based SVM kernel, the agent will receive the anomaly traffic to perform further analyses.

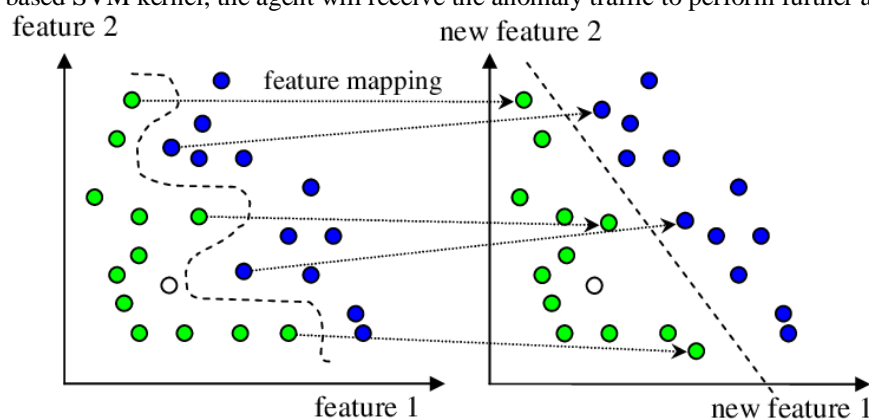


Figure 4. The kernel function in SVM.

The observations involve three examples, normal, anomaly, and DDoS traffics, as well as the agent's response for all three instances. The parameters of the traffic anomaly are categorised to be unusual according to the traffic stable, continuous, and discrete as can be seen in Table 1. The attack type can be sorted through this classification.

Table 1. Scenario Setting

Traffic conditions	Req.	Behavior
Normal	50018	stable
Anomaly	117359	discrete
DDoS	18627	continuous

Moreover, three cases have been selected from the simulation implementation. The first case shows the system performance when there is no attack traffics have been detected as shown in Fig. 5.



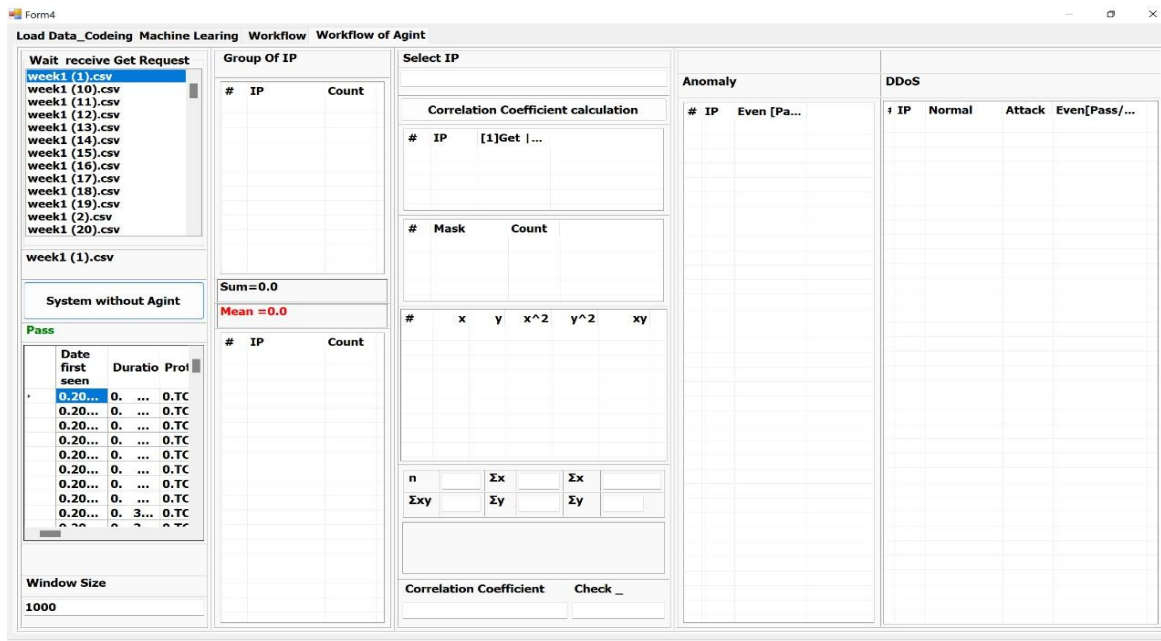


Figure 5. The performance of the proposed system at the first case

Whereas, the second case shows the performance of the proposed system when an abnormal traffics with a small number of requests have been detected. These traffics have been matched with the threshold and according to the traffics behavior, the system classified it as an abnormal traffics as shown in the bellow Fig. 6.

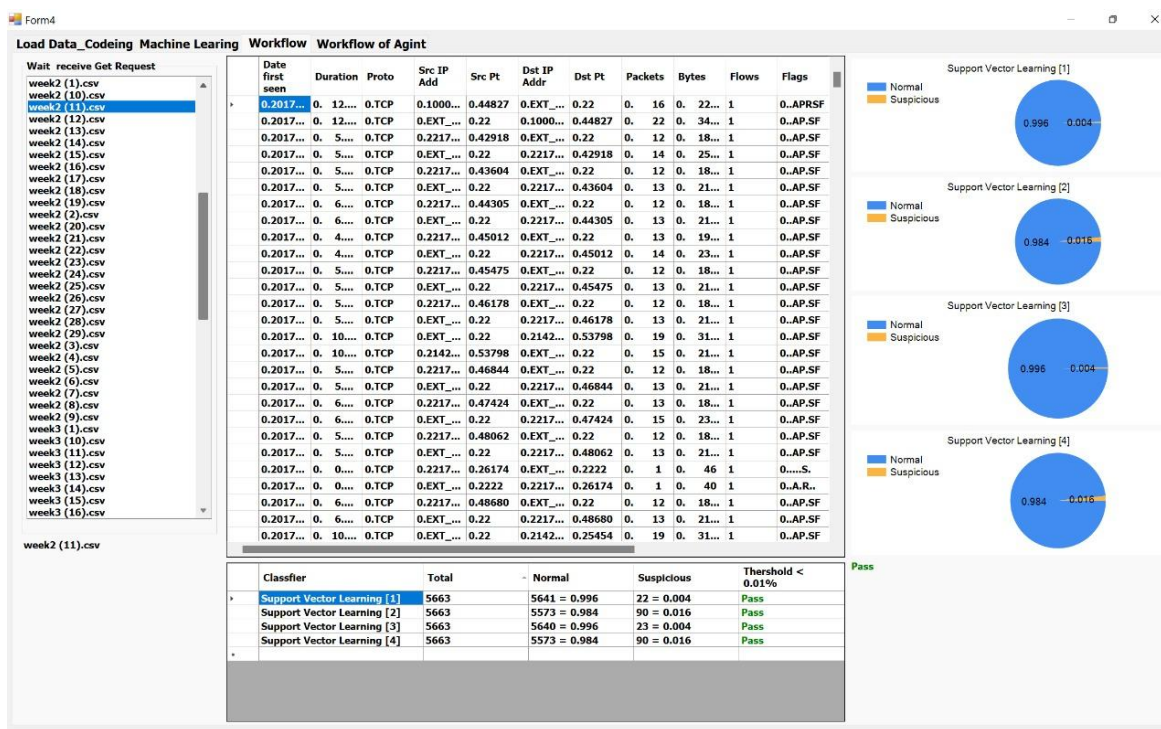


Figure 6. The performance of the proposed system at the second case

Furthermore, the third case shows the performance of the proposed system when an attack traffics with a large number of requests have been detected. However, the incoming traffics is more than the threshold it means there is abnormal traffics, and it may belong to the attacker or it is normal traffics but more than the threshold. In the case of attack traffics the agent will send the traffics for permanent block in the bloom filter. Whereas, in the second case of the agent will sent the traffic to the Kalman filter for



temporary block. These traffics have been matched with the threshold and according to the traffics behavior, the system classified it as an attack traffics as shown in the bellow Fig. 7.

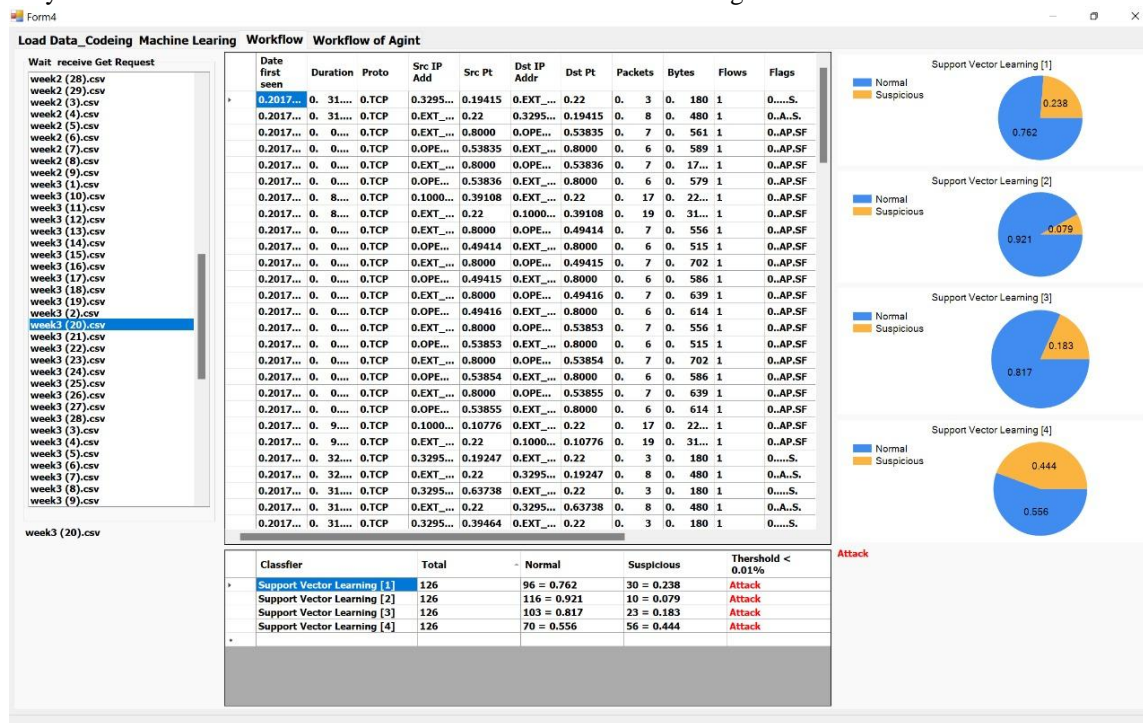


Figure 7. The performance of the proposed system at the second case

In Fig. 8, the graph offers descriptions of the number of anomaly requests for the fourth week from the dataset selected to pass through the first stage in the proposed system. Also, it was noticed that there was a minor increase in traffic on the second day. Then, the cumulative number of requests for further analysis was sent to the second function of the agent.

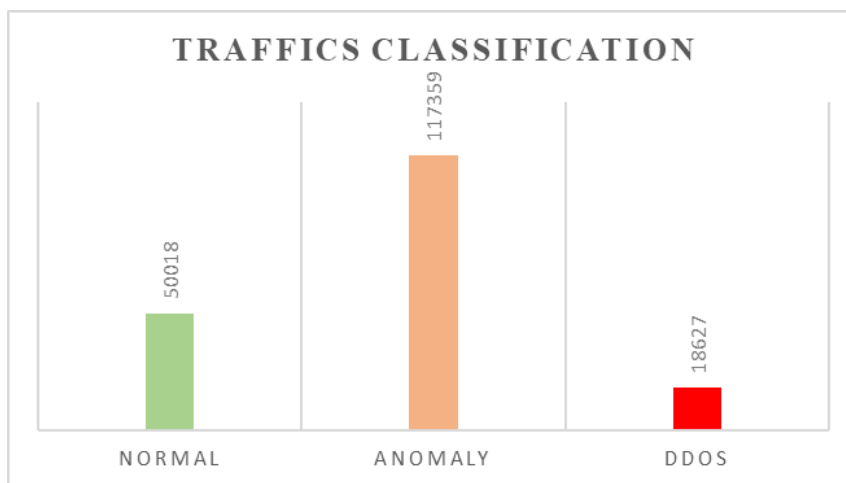


Figure 8. Average of classified traffics for the Anomaly Traffics for the testing dataset at Agent stage

Figure 8 displays the sum of attack requests from the selected data set for the fourth week from the agent. The agent is employed to break attack traffic between the DDoS and the abnormal based on traffic actions, then to apply the abnormal traffic for further analysis into Kalman filter and DDoS traffic at the adaptive agent. However, the proposed model produced an excellent performance in DDoS attacks and abnormal traffics with accuracy of 99.6% The proposed model is therefore distinguished it self from the related work in that the assumption and sensitivity of DDoS attack and abnormal flood detection have been determined.



6. DISCUSSION

A disruptive incident that does not require internal system access is a danger to DDoS. It's often difficult to detect in the early stage. This involves the deployment of a significant number of zombies, who are at risk of possible injury. A majority of nodes were redirected to a particular goal by the critical forms of the attack, which may have catastrophic effects for its victims and plague the networks. There is another form of traffic flooding, the abnormal. Abnormal traffic is defined as a type of network traffic comparable to DDoS traffic but originating from legitimate users. It is a traffic like a DDoS attack, which enables multiple illegitimate users to reach the website at the same time. Several techniques have been formulated, built, and applied to defend application layer countering DDoS cyberattacks. Nevertheless, the hidden malicious traffic which are concealed through genuine traffic and also abnormal traffics appears to be a general scourge in these protection models. It can not readily discriminate between actual traffic and deceptive traffic basis on negative performance and false positives. The research proposed, implemented, evaluated, and contrasted with the results of the proposed model revealed that the proposed model was effective in the protection against DDoS attacks targeting application layer.

By comparing the proposed model with related work of Ojugo Arnold, [14], Chauhan and Heydari, [13], and Saad, et al [15] it is observed that the proposed system achieved the best accuracy of 99.6%. The dataset is segmented to 60 percent of the dataset was used in model training, while the remaining 40 percent was used to test the model based on the sigmination in the related work. A comparison of the proposed model is rendered based on the dataset slicing setup.

The model, though, differs from previous methods by utilizing the decision module, which utilizes the agent to modify and recognize the DDoS and the abnormal flood traffic. The agent responds differently to each of the attacks with different forms of filtering behavior. The comparison results are presented in Table 2. It can be observed from this table that, compared to other simulations utilizing the same dataset, the overall accuracy of the proposed model was 99.6%.

Table 2. The performance of the Proposed Model according to the Related Work

Model	Accuracy
Ojugo Arnold, [13]	98.8%
Chauhan and Heydari, [14]	98.8%
Saad, et al [15]	98.8%
Proposed model	99.6%

7. CONCLUSION

DDoS attack is one of the most dangers type of attack that targeting could computing environment and consume it is resources. In this work, a Defense of Flooding Attacks model has been proposed for securing could environment against DDoS attack. A hybrid of SVM and agent have been performed to classify, recognize and filter the anomaly traffics. The proposed system is applicable at could computing environment, IoT, and the devices which has internet concoctions. In order to test and evaluate the performance of the proposed model, CIDDS 2017 dataset was used. The proposed system achieved an excellent result during the comparison with the related work. In the future work, testing the proposed system in real environment is recommended.

Acknowledgement

Husam Saleh Mahmood is sincerely thanked to Profs: Dr.Guirguis, Dr. El-sayed, and El-sayed El-morsy for their insightful comments and suggestions that helped significantly improve this research work.

REFERENCES

- [1] B. A. Khalaf *et al.*, "A simulation study of syn flood attack in cloud computing environment," *AUS journal*, vol. 26, no. 1, pp. 188-197, 2019, DOI:[10.11591/eei.v10i1.2516](https://doi.org/10.11591/eei.v10i1.2516).
- [2] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *2017 3rd international conference of cloud computing technologies and applications (CloudTech)*, 2017: IEEE, pp. 1-7, DOI: [10.1109/CloudTech.2017.8284731](https://doi.org/10.1109/CloudTech.2017.8284731).
- [3] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, 2012: IEEE, pp. 1-5, DOI: [10.1109/SCEECS.2012.6184829](https://doi.org/10.1109/SCEECS.2012.6184829).
- [4] V. Farhat, B. McCarthy, R. Raysman, and J. Canale, "Cyber attacks: prevention and proactive responses," *Practical Law*, pp. 1-12, 2011, <https://www.hklaw.com/files/Uploads/Documents/Articles/2017/CyberAttacksPreventionandProactiveResponses.pdf>.
- [5] P. Suresh, "Survey on seven layered architecture of OSI model," *International Journal of research in computer applications and robotics*, vol. 1, pp. 1-12, 2011, DOI: [10.1109/IJCARR.2011.5618292](https://doi.org/10.1109/IJCARR.2011.5618292).



- 4, no. 8, pp. 1-10, 2016, https://www.ijrcar.com/Volume_4_Issue_8/v4i801.pdf.
- [6] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1985-1997, 2019, DOI: <https://doi.org/10.1007/s12652-018-0800-9>.
- [7] S. Mugunthan, "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing," *J. Soft Comput. Paradig.(JSCP)*, vol. 1, no. 02, pp. 80-90, 2019, DOI: <https://doi.org/10.36548/jscp.2019.2.003>.
- [8] S. Potluri, M. Mangla, S. Satpathy, and S. N. Mohanty, "Detection and prevention mechanisms for DDoS attack in cloud computing environment," in *2020 11th international conference on computing, communication and networking technologies (ICCCNT)*, 2020: IEEE, pp. 1-6, DOI: [10.1109/ICCCNT49239.2020.9225396](https://doi.org/10.1109/ICCCNT49239.2020.9225396).
- [9] T. Karnwal, S. Thandapanii, and A. Gnanasekaran, "A filter tree approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in *Intelligent informatics*: Springer, 2013, pp. 459-469, DOI: [10.1007/978-3-642-32063-7_49](https://doi.org/10.1007/978-3-642-32063-7_49).
- [10] I. Sattar, M. Shahid, and Y. Abbas, "A review of techniques to detect and prevent distributed denial of service (DDoS) attack in cloud computing environment," *International Journal of Computer Applications*, vol. 115, no. 8, 2015, DOI: [10.5120/20173-2370](https://doi.org/10.5120/20173-2370).
- [11] D. Juneja, R. Chawla, and A. Singh, "An agent-based framework to counter attack DDoS attacks," *International Journal of Wireless Networks and Communications*, vol. 1, no. 2, p. 193, 2009, <http://www.ripublication.com/ijwnc.htm>.
- [12] M. A. Alarqan, Z. F. Zaaba, and A. Almomani, "Detection mechanisms of DDoS attack in cloud computing environment: A survey," in *International Conference on Advances in Cyber Security*, 2019: Springer, pp. 138-152, DOI: [10.1007/978-981-15-2693-0_10](https://doi.org/10.1007/978-981-15-2693-0_10).
- [13] R. Chauhan and S. S. Heydari, "Polymorphic Adversarial DDoS attack on IDS using GAN," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020: IEEE, pp. 1-6, DOI: [10.1109/ISNCC49221.2020.9297264](https://doi.org/10.1109/ISNCC49221.2020.9297264).
- [14] A. A. Ojugo and R. E. Yoro, "Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 2, p. 1498, 2021, DOI: [10.11591/ijece.v11i2.pp1498-1509](https://doi.org/10.11591/ijece.v11i2.pp1498-1509).
- [15] R. M. Saad, M. Anbar, S. Manickam, and E. Alomari, "An intelligent icmpv6 ddos flooding-attack detection framework (v6iids) using back-propagation neural network," *IETE Technical Review*, vol. 33, no. 3, pp. 244-255, 2016, DOI: <https://doi.org/10.1080/02564602.2015.1098576>.
- [16] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Computer Networks*, vol. 81, pp. 308-319, 2015, DOI: <https://doi.org/10.1016/j.comnet.2015.02.026>.
- [17] A. R. Wani, Q. Rana, U. Saxena, and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," in *2019 Amity International conference on artificial intelligence (AICAI)*, 2019: IEEE, pp. 870-875, DOI: [10.1109/AICAI.2019.8701238](https://doi.org/10.1109/AICAI.2019.8701238).
- [18] A. Kenyon, L. Deka, and D. Elizondo, "Are public intrusion datasets fit for purpose characterising the state of the art in intrusion event datasets," *Computers & Security*, vol. 99, p. 102022, 2020, DOI: <https://doi.org/10.1016/j.cose.2020.102022>.
- [19] G. S. Kushwah and V. Ranga, "Detecting DDoS Attacks in Cloud Computing Using Extreme Learning Machine and Adaptive Differential Evolution," *Wireless Personal Communications*, pp. 1-24, 2022, DOI: <https://doi.org/10.1007/s11277-022-09481-9>.
- [20] D. M. Abdullah and A. M. Abdulazeez, "Machine learning applications based on SVM classification a review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 81-90, 2021, DOI: <https://doi.org/10.48161/qaj.v1n2a50>.
- [21] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abdulllah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of






- service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691-51713, 2019, DOI: [10.1109/ACCESS.2019.2908998](https://doi.org/10.1109/ACCESS.2019.2908998)
- [22] A. Zuhilmi, S. A. Mostafa, B. A. Khalaf, A. Mustapha, and S. S. Tenah, "A comparison of three machine learning algorithms in the classification of network intrusion," in *International Conference on Advances in Cyber Security*, 2020: Springer, pp. 313-324, DOI:https://doi.org/10.1007/978-981-33-6835-4_21.
- [23] J. N. Hasoon, B. A. Khalaf, R. S. Hameed, S. A. Mostafa, and A. H. Fadil, "A Light-Weight Stream Ciphering Model Based on Chebyshev Chaotic Maps and One Dimensional Logistic," in *International Conference on Advances in Cyber Security*, 2021: Springer, pp. 35-46, DOI:https://doi.org/10.1007/978-981-16-8059-5_3.
- [24] V. de Miranda Rios, P. R. Inácio, D. Magoni, and M. M. Freire, "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks*, vol. 186, p. 107792, 2021, DOI: <https://doi.org/10.1016/j.comnet.2020.10.7792>
- [25] B. A. Khalaf *et al.*, "An adaptive protection of flooding attacks model for complex network environments," *Security and Communication Networks*, vol. 2021, 2021, DOI: <https://doi.org/10.1155/2021/5542919>

BIOGRAPHIES OF AUTHORS

	<p>Husam Saleh Mahmood    received the B.Sc. of Computer Science from Dept. of Computer Science - College of Science / Alyarmok University Collage, Iraq, and currently, I am studying a M.Sc. in Mathematics and Computer Science from Alexandria University, Egypt. He can be contacted at email: Hussam.saleh_PG@alexu.edu.eg</p>
	<p>Shawkat Kamal Guirguis    is Professor of Computer Science & Informatics, Information Technology Dept., Institute of Graduate Studies & Research (IGSR), Alexandria University (Since Dec. 2006-current), he received B.Sc. & M.Sc. of Computer Science & Automatic Control from Faculty of Engineering, Alexandria University, Egypt, and Ph.D. Electronics & Communication, Co-Supervised by Cairo University, and Imperial College of Science & Technology, University of London, U.K., He is participated in teaching computer science courses and supervising graduate projects for successive years in the Arab Academy for Science and Technology and Maritime Transport, He participated in developing two lab accreditation projects (Air lab and Water Lab) as well as the CIQAP project His research interests include of Computer Science & Automatic Control. He can be contacted at email: shawkat_g@alexu.edu.eg, Shawkat_g@yahoo.com</p>
	<p>Wagdy Gomaa El-sayed    is a Professor of pure mathematics, Faculty of science, Alexandria University. His research interests include of Mathematics, Computer Science, Biochemistry, Genetics and Molecular Biology, Engineering. He can be contacted at email: wagdygoma@alexu.edu.eg,</p>





Shaimaa Elmorsy    is Lecturer of Computer and Data Science, Alexandria University, Alexandria, Egypt. She received B.Sc., M. Sc, and Ph.D. of Computer Science from Alexandria University, Egypt. Her research interests include of Data structure, Python, Robotics, Operating system, Computer Architecture. She can be contacted at email: shaimaa.aly.comp@alexu.edu.eg.

