Collaborative Cloud IDS in Detecting Denial of Service by Dendritic Cell Mechanism

Azuan Ahmad[1], Mohd Nazri Kama[2], Azri Azmi[2], and Norbik Bashah Idris[3]
[1] Faculty of Science and Technology, Universiti Sains Islam Malaysia, Malaysia
[2] Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia
[3] Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia
Email: azuan@usim.edu.my; {mdnazri; azriazmi}@utm.my; norbik@uuim.edu.my

***Abstract*—The term Cloud computing is not new anymore in computing technology. This form of computing technology previously considered only as marketing term, but today Cloud computing not only provides innovative improvements in resource utilisation but it also creates a new opportunity in data protection mechanisms where the advancement of intrusion detection technologies are blooming rapidly. From the perspective of security, Cloud computing also introduces concerns about data protection and intrusion detection mechanism. This paper aims to provide Denial of Service (DoS) detection for Cloud computing environment. As a result, we provide an experiment to examine the capability of the proposed system. The result shows that the proposed system was able to detect all types of attacks that conducted during the experiment. We conclude the paper with a discussion on the results, then we include together with a graphical summary of the experiment's result.**

***Index Terms*—cloud computing, information security, artificial immune system, intrusion detection, dendritic cell, denial of service**

I. Introduction

Cloud computing is the new concept of computing where people only need to pay for services and resources without needed to place any cost for physical hardware [1]. With the implementation of Cloud computing in the application today, it emerges a new technique in software development and deployment. It also changes how people are using and managing resources. Cloud computing can be defined as internet-based computing, where shared resource, software and information are provided to the user on demand [2].

Cloud computing systems are distributed and nesting a lot of resources and private information, therefore because of their nature, cloud computing environments are easy targets for intruders looking for possible vulnerabilities to exploit [3]. When organizations and companies which are using Cloud computing services, they will move their resources from their own private infrastructure to the Cloud infrastructure. If the Cloud is compromised, the organization's resource will be at risk. Cloud Computing systems need protection mechanisms that will monitor the network activity and detect if any intrusion attempts happen within the Cloud Computing infrastructure whether it was from external or internal sources [4]. In fact, the cheap availability of significant amounts of computational resources can be regarded as a means for easily perpetrating distributed attacks, as it has recently been observed in several security incidents involving Amazon's EC2 cloud infrastructure [5].

One of the risk affecting Cloud computing environments is Denial of Service (DoS) attack. Before this, DoS attack focused on taking down any target including servers, hosts or devices by flooding the targets with huge amount of data in a manner such that the service become unavailable due to a large number of request. As Cloud become popular and pools huge amount of resources, attackers start to target Cloud environment as a DoS victim. Authors in [6] show a strong anticipation about the Distributed Denial of Service (DDoS) attackers target shift towards cloud infrastructure and services. More than 20% of enterprises in Malaysia saw at least one reported DDoS attack incident on their infrastructure [7]. Many attacks in last two years support these attack anticipations presented in the report.

Amongst many recent attacks, there are few popular attacks which gained a lot of attention in the research community [8]. Lizard Squad attacked cloud-based gaming services of Microsoft and Sony which took down the services on Christmas day. Cloud service provider, Rackspace, was targeted by a massive DDoS attack on its services. In another spectacular attack example, Amazon EC2 cloud servers faced another massive DDoS attack. These attack incidents incurred heavy downtime, business losses and many long-term and short-term effects on business processes of victims. A report by Verisign Defense Security Intelligence Services shows that the most attacked target of DDoS attacks in the last number of quarters is cloud and SaaS (Software as a Service) sector.

The main objective of this paper is to propose a real-time working algorithm based on Dendritic Cell Algorithm (DCA) in detecting DoS in Cloud computing environment and to study the ability of the proposed DCA in detecting DoS within Cloud network environment. A review of the literature shows that there is lacking work on the detection of DoS in Cloud

Manuscript received November 10, 2018; revised February 14, 2019; accepted February 14, 2019.
Corresponding author: Azuan Ahmad (email: azuan@usim.edu.my)

doi: 10.18178/ijeetc.8.4.188-193

computing that focused on implementing Artificial Immune System (AIS) and in the meantime, research in DCA still lacking in developing real-time anomaly DoS detections. For this purpose, an algorithm is proposed in this paper to provide a new real-time DoS detection mechanism which works on Cloud based on DCA.

II. Related Works

This section reviews the previous work related to DoS detection in Cloud research and prototypes. The number of research focusing in Cloud DoS detection is increasing rapidly in recent years and there are several solutions that researchers proposed to solve the issues in Cloud Security.

Distributed Cloud IDS introduced [9] supports an idea of cooperative defence by IDSs in the cloud computing environments by deploying IDS in each cloud computing region and exchange alert with each other. Their proposed system was tested with custom Denial of Service (DoS) attack targeting the Cloud network and the results show that their proposed system provides 97% detection rate. Their works a suspect to suffer from any new attacks because they only rely on signature-based IDS.

The recent work from [10] introduces dendritic cell algorithm in intrusion detection against cloud computing environment. This work used DARPA 99 datasets for learning and testing with 60% of accuracy. However, the dataset used with this experiment considered outdated and the result may vary depends on using recent datasets.

Cloud Trace Back (CTB) model proposed by [11] protects cloud environment from Distributed Denial of Service (DDoS) by using Trace Back model specified for Cloud computing. Their model finds the source of DDoS attacks and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic. From the experiment CTB can classify DoS attack to around 75% detection rate.

The work from [12] proposed an entropy based detection technique that uses packet dropping mechanism to detect DoS attack on cloud computing environment. The entropy rate is used to identify attack flow based on the distribution ratio. The proposed system is deployed on each edge router which subsequently transfers the flow to an adjacent router for a confirmatory check when DoS is detected. If confirmed, DoS packets are dropped. Findings from the simulation shows a detection rate of 90%.

In other work, Modi [13] propose a profile based network intrusion detection and prevention system that secures the cloud against DoS attack. It combines both data analysis and Bayesian technique to detect DDoS attacks using unsupervised learning algorithm.

The latest work from [14] implemented finite state Hidden Markov Model (HMM) in predicting multi stage attack in detecting network based attack. They include HMM as an improvement from their previous work for predicting and provides early warning for any future attacks. Their proposed system works by tracking the evolution of an attack while it is still in progress and then the system can activate suitable actions based on a confidence level threshold. This model has successfully detected the attack in the experiment by 39 minutes plus 37 seconds and 64 minutes plus 42 seconds earlier before the detection phase starts.

Reference [15] proposed an Host-based Intrusion Detection System (HIDS) based on intrusion severity analysis for cloud computing where in their research, they used the hybrid approach where the attack were detected based on the attack database that they provide and from the Profile Engine (PE) which is based on the behaviour of the monitored Virtual Machines (VM). This machine learning based IDS using classification technique for intrusion severity analysis from the monitored system calls. The dataset used in this research is the artificial data generated from the computer program. This dataset did not provide the real cloud environment and did not represent the actual response of a cloud environment towards any attack. The results obtained from the research successfully demonstrate the effectiveness of the intrusion severity analysis method for Clouds but the dataset and may be questionable because the research used the self-generated dataset and they did not provide details about the methodology in building their datasets.

Work from [16] using SU-Genetic algorithm in detecting intrusions in Cloud computing environment especially in SaaS model. Their proposed GA engine analysed data and matched the data with the signature database in the detection engine. This system monitors the intrusions by matching the signature in the knowledge database. The SU-Genetic method ranks features by the symmetrical uncertainty and then selects features with the genetic algorithm. The correlation evaluator with SU value is applied in genetic selection to balance the correlation and redundancy. After experimented on the NSL-KDD dataset, the features were reduced from 41 to 17 and the amount of data was roughly reduced to 41% of the original.

III. Artificial Immune System

A long-term goal of the security community has been to create an 'immune system' for information systems with the flexibility, effectiveness and robustness of the immune system that protects organisms. A system that can respond effectively to new threats with minimal or no human interaction would significantly improve the security of Cloud computing environment.

Artificial Immune Systems (AIS) offer a means to solve complex, dynamic problems like many of those found in the domain of information security [17]. AIS refer to a group of computational intelligence techniques that are inspired by the information processing capabilities of the human immune system (HIS). These systems are effective at anomaly and signature-based detections and shows promising results in detecting novel threats.

AIS research starts with the work of [18] which introduces Negative Selection Algorithm (NSA) as an intrusion detection algorithm inspired by the negative selection process of B-cells and T-cells in antibody

generation process. NSA had been applied in various areas including virus detection [19] and IDS [20]. With respect to the research on IDS, this anomaly detector-like feature of AIS attracted a growing number of computer scientists and they have proposed several different computer immune models such as Gene Library Evolution [21], Clonal Selection [22], Danger Theory [23], Immune Memory [24] and Dendritic Cell Algorithm (DCA) [25].

In HIS, there are cells that building a bridge between adaptive and innate immune system called Dendritic Cells (DC). DC acts as the evidence collector that collecting signals and antigens found in the cytokines at the area of the cells was located. After the cells achieve their maturation threshold, the cells then migrate to lymph node and interact with T-cells and B-cells to initiate or suppress adaptive immune response depends on the state of their maturation whether mature or semi-mature. Based on the natural properties of DC, it has a huge potential in real world problem solving such as detecting intrusions in Cloud computing environment. The work of [25] proposed Dendritic Cell Algorithm (DCA) which inspired by the characteristics of DC and provides solutions for previous AIS auto-immunity problems [26]. Since then, number of research in DCA increased and developed very fast. Some of the works that always being highlighted are detecting SYN scan attack, botnet detection [27] and hybrid DCA [28]. However, not many research focused on the practical implementation of DCA in detecting intrusions for real environment in Cloud computing [29].

A. Dendritic Cell Inspirations

This section discussed about Dendritic Cell (DC) in general which is the inspiration for the development of the algorithm and followed with the proposed cloud Denial of Service (DoS) detector which is an algorithm derived from DC and to show the contributions of this paper.

Dendritic cells are the main function in natural immune system by which the innate immune system collects and present antigens to the adaptive immune system for processing. Dendritic cell exist within three states immature, semi-mature and mature dendritic cell where immature dendritic cells are reside in tissues throughout the body for collecting antigens and signals for processing, semi-mature dendritic cells is the results from immature dendritic cells that collect antigen and signal in an environment that have safe signal more than danger signal and mature dendritic cell on the other hand is the results from immature dendritic cells that collect antigen and signal in an environment that have danger signals more than safe signals. Dendritic cells are especially abundant in tissues where pathogens may enter body, such as skin, lung and gastrointestinal tract.

B. Dendritic Cell Algorithm

The Dendritic Cell Algorithm (DCA) introduced by [25] inspired by the function of natural Dendritic Cell (DC) as explained in previous section. DCA has the ability to analyse multiple signals and produce the current context of the environment. The correlation between context and antigen become a basis for anomaly detection in this algorithm. Motivated by the human immune system, three signals are defined for the input signals of the algorithm in general known as Danger, Safe and PAMP signals. If we make use the signal in anomaly intrusion detection, the semantics of each signals would be as in Table I.

TABLE I. SEMANTICS OF DCA SIGNALS

Signals	Semantics
PAMP	Indicate the presence of definite anomaly
Safe	Indicate the presence of absolute normal
Danger	May or may not be a sign of the occurrence of anomaly, but the likelihood of being anomalous is rising as the value increases.

Based on the pre-defined weight, DCA generates three output signals known as Mature, Semi-mature and co-stimulation signal (CSM). Equation 1 displays the computation of output signals introduced by [25].

$$O_{ip} = \sum_{j=0}^{2} S_{ij} W_{jp}$$

where i is the sequence numbers of the sampled antigens in the dataset (Antigen ID); j=0, 1, 2 are the three input signals of PAMP, DS, SS; p=0, 1, 2 are the three output signals of CSM, Semi-Mature, Mature; O_{ip} is the p output signal concentration of the i antigen; S_{ij} is the j input signal concentration of the i antigen; and W_{jp} is the transforming weight from S_{ij} to O_{ip}.

The output signals will indicate the level of anomaly in the monitoring area. Dendritic cell in the monitoring process will produce co-stimulatory (CSM) signals. In the danger or unhealthy tissue environment, the dendritic cell will produce a large amount of mature signal and in the safe or healthy environment, the dendritic cell produce semi-mature output signal. In the brief explanation, an individual DC total out the output signals over time, resulting in cumulative CSM, cumulative semi-mature and cumulative mature. This procedure continues until the cell achieves the completion of its lifespan, where the cumulative CSM exceeds the migration threshold, the DC stop to sample signals and antigens.

At this point, the remaining cumulative signals are measured. If the cumulative Semi-mature is larger than the cumulative Mature value, the cell mutates to semi-mature state and is assigned a ‘context value’ of 0, and if the cumulative Mature value was greater it will influence the maturation towards mature state and a context value of 1. To measure the possible anomalous level of an antigen, a coefficient is derived from the aggregate values across the population, termed the Mature Context Antigen Value (MCAV) of that antigen. This is the proportion of mature context presentations (context value of 1) of that particular antigen, relative to the total amount of antigens presented. This results in a value between 0 and 1 to which a threshold of anomaly, termed ‘MCAV threshold’, may be applied. The chosen value for this threshold reflects the distribution of normal and anomalous items presented within the original dataset.

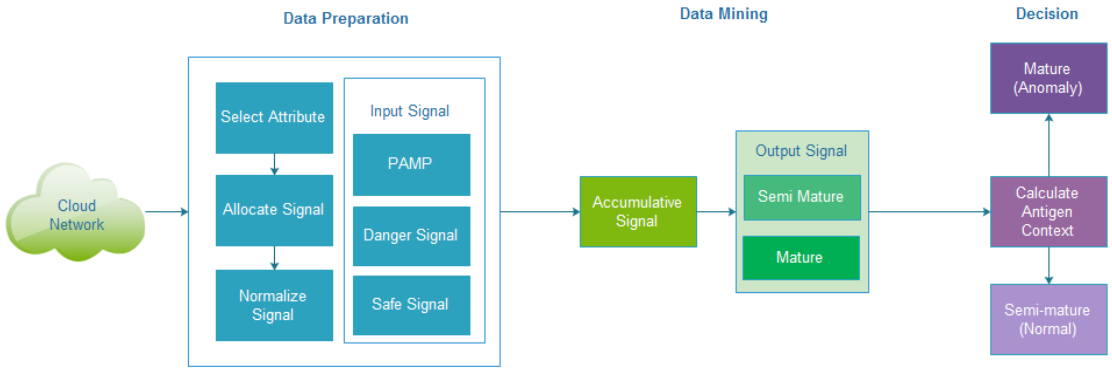

Fig. 1. Modified DCA model for cloud computing environment.

Once this value has been applied, antigens with a MCAV which exceeds this threshold are classified as anomalous and vice versa. To clarify the algorithm a graphical illustration was presented in Fig. 1.

IV. Proposed Cloud Denial of Services Detector

Each monitored Cloud network activity is viewed as Antigen and the Internet Protocol (IP) address of each packet is taken as the Antigen identity. The CDoSD perform multiple signals and antigens sampling. CDoSD model will collect three signals from the Cloud environment; PAMP, Safe Signal and Danger signals linked to a specific antigen that trigger that signals. More details on the signals generation are explained in the following section.

The signals then will be cumulatively group based on the DC. In our experiment, we consider each DC handles a specific antigen. Based on the collected input signals, the DC will be transform into either three outputs states; co-stimulatory signal (CSM), semi-mature and mature. When the DC exceeds the maturation threshold, in our case the monitoring time limit, the DC stop monitoring, and the output signal values will be analysed. When learning ends, antigens appear in the value of mature and semi mature. In the last step, the potential anomalous antigen is determined based on the collected context as decided based on the antigens with greater mature value are classified as anomalous group while the opposite is considered as the normal category.

A. Improvement of Cloud Denial of Services Detector

Running Cloud Denial of Services Detector (CDoSD) in a Cloud environment limits the processing power reserved for DoS detection. It is because the Cloud implements resource pooling which is the pool of resources is shared together among multiple Cloud host. This requires the DCA to be modified to fit the Cloud environment as explained within this section. The aim of the modification is to minimise the processing by CDoSD at the same time provide reliable DoS detections. Single cell model is the solution proposed for performance improvement in DoS detection.

B. Single Cell Model

As original DCA requires multiple instances of cells population to be analysed before the Mature and Semi-mature states can be decided, we believe that this process can be simplified by using Single Cell model to reduce the additional processing and reduce delay in multiple cell colleting processes during the online real-time analysis. This model first described in Oates et al work [30]. The model in this research focused on a behavioural level of a single DC for a specified time space. Each DC events in each state are depending on a particular time interval. Each DC will be in either Mature or Semi-mature states at the end of the time interval. This modification is suitable in enhancing DCA for real-time intrusion detection in Cloud environment.

The original DCA develops the cell population by multiplying each cell by certain number of cell size and measures the MCAV values. If the MCAV value exceeds the threshold value, then the cell population is considered in a mature state and vice versa. This process did not suitable in our implementation which requires real time results and analysis. As a solution, we simplify the process by using single cell approach where each antigen and signals is not divided into cell population, but the decision of mature and semi-mature were measured based on comparison between preliminary mature and semi-mature value on each time frame. For a time frame that having the mature value more that semi-mature, the event were considered Mature or in other term malicious state and in the other hand, were considered Semi-mature or safe state.

V. Experiment

Testing the performance of CDoSD model is crucial in measuring the ability the CDoSD in detecting DoS. This section explained the experiment conducted in measuring the ability of CDoSD in detecting DoS. This experiment was conducted using ISCX 2012 Dataset that will be explained in detail in the following subsection.

A. ISCX 2012 Dataset

For the experiment, the ISCX 2012 Intrusion Detection Evaluation dataset was used to evaluate the performance of CDoSD in detecting DoS. ISCX 2012 dataset consist of seven days of recorded network traffic which three days contains only normal network activities while the remaining contains multiple types of attacks as summarises in Table II below:

TABLE II. ISCX 2012 INTRUSION DATASET DESCRIPTIONS

Date	Description
Friday, 11/6/2010	Normal Activity
Saturday, 12/6/2010	Normal Activity
Sunday, 13/6/2010	Infiltrating the network from inside + Normal Activity
Monday, 14/6/2010	HTTP Denial of Service + Normal Activity
Tuesday, 15/6/2010	Distributed Denial of Service using an IRC Botnet
Wednesday, 16/6/2010	Normal Activity
Thursday, 17/6/2010	Brute Force SSH + Normal Activity

For this experiment, we only interested on the 14/6/2010 record since the data set contains only HTTP DoS attacks or normally called Slowloris attack. This single day dataset contains 9,648,000 number of packets with 20 features.

For the detection of DoS attack using ISCX 2012 dataset, six signals were derived from behavioural attributes of the monitored victim cloud host: one PAMP, three danger signals and two safe signals. The PAMP signals is collected from data source which obviously indicate an attack which is the alert from the signature-based Intrusion Detection System (IDS) installed within the CDoSD. Danger signals (DS-1, DS-2 and DS-3) are extracted from attributes which represent changes in behaviour in this case, extracted from the network flow rate, memory status and processing performance of the monitored environment. Safe signals (SS-1 and SS-2) are also taken from changes in behaviour but high safe signal values are collected from a normal behaviour condition which is derived from the normal network flow, normal memory and processing performance. All signals are normalised using z-score normalisation within a range of 0 to 100.

We built a private cloud environment using Kernel-based Virtual Machine (KVM) with four cloud host and one monitoring host. The monitoring host was installed with Network-based Intrusion Detection System (NIDS) and in a mirror mode where all network traffic for other cloud host will be mirrored towards monitoring host. The packets of ISCX 2012 dataset were replayed into the test bed cloud environment and the reaction from each host were monitored using Zabbix network monitoring tool. The signals secreted from each host were collected and analysed to produce the danger and safe signal level. Based on this signal, the condition for each cloud host were sumamrised based on the signal level. High danger signal level indicated that the cloud host were in an unhealthy condition and on the other hand, high level of safe signals is a healthy indicator for monitored cloud host.

VI. RESULTS & DISCUSSIONS

This section discussed the results from the experiments conducted as explained in previous section. The experimental result for DoS detection using ISCX 2012 dataset are summarised in Table III. Table III representing measurement in terms of true positive, false positive, false negative, detection rate and false alarm rate. From Table III, the CDoSD has produced a slightly high detection rate with low false alarm rate 94.4% and 5.04% respectively.

TABLE III. ISCX 2012 EXPERIMENT RESULT

True Positive	False Positive	False Negative	Detection Rate	False Alarm
4328	746	256	94.4	5.04

Further comparisons were made with other methods and the results are shown in Table IV. All previous research also tested their method on DoS detection in Cloud environment. It is clear that CDosD perform high improvement in detection rates especially among anomaly-based detection research on cloud DoS detection.

TABLE IV. COMPARISON OF CDOSD WITH PREVIOUS FINDINGS

Approaches	Detection Rate (%)
CDoSD	94.4
DIDS [9]	97
CTB [10]	75
Entropy Based [11]	90
Profile Based [12]	91

VII. CONCLUSION

In this paper, a modified Dendritic Cell algorithm was proposed to provide a solution in detecting DoS targeting the Cloud environment. This modified algorithm was applied in a prototype named Cloud Denial of Service Detection (CDoSD) and tested with ISCX 2012 dataset. All of the experiments were conducted to measure the ability of CDoSD in detecting DoS attacks. The result shows that the CDoSD was able to detect 94.4% of DoS attacks in the dataset. Based on the result, we can summarise that the modified DCA was able to bring a new solution in providing security to Cloud computing environment.

ACKNOWLEDGEMENT

This project is funded by Ministry of Higher Education (MoHE) under Fundamental Research Grant Scheme (FRGS), vote number: 4F861.

REFERENCES

[1] Q. Jiang, J. Ma, and F. Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 12, no. 2, pp. 2039–2042, Jun. 2018.

[2] R. Varatharajan, G. Manogaran, and M. K. Priyan, "A big data classification approach using LDA with an enhanced SVM method for ECG signals in cloud computing," *Multimed. Tools Appl.*, vol. 77, no. 8, pp. 10195–10215, Apr. 2018.

[3] C. Kaleeswari, P. Maheswari, K. Kuppusamy, and M. Jeyabalu, "A brief review on cloud security scenarios," *Int. Journal of Scientific Research in Science and Technology*, vol. 4, no. 5, pp. 46-50, Mar. 2018.

[4] D. Dave, N. Meruliya, T. D. Gajjar, G. T. Ghoda, D. H. Parekh, and R. Sridaran, "Cloud security issues and challenges," in *Big Data Analytics*, V. Aggarwal, V. Bhatnagar, D. Mishra, Eds., Singapore: Springer, 2018, pp. 499–514.

[5] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, Jan. 2018.

[6] N. Agrawal and S. Tapaswi, "Low rate cloud DDoS attack defense method based on power spectral density analysis," *Inf. Information Processing Letters*, vol. 138, pp. 44-50, Oct. 2018.

[7] M. R. Haque, *et al*., "Analysis of DDoS attack-aware software-defined networking controller placement in Malaysia," in *Recent Trends in Computer Applications*, Springer, Jan. 2018, pp. 175–188.

[8] D. Chaudhary, K. Bhushan, and B. B. Gupta, "Survey on DDoS attacks and defense mechanisms in cloud and fog computing," *Int. Journal of E-Services and Mobile Applications*, vol. 10, no. 3, pp. 61–83, 2018.

[9] P. Sharma, J. Sengupta, and P. K. Suri, "WLI-FCM and artificial neural network based cloud intrusion detection system," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 1, pp. 3698–3703, Jul. 2018.

[10] N. B. I. A. Ahmad and M. N. Kama, "CloudIDS: Cloud intrusion detection model inspired by dendritic cell mechanism," *Int. J. Commun. Networks Inf. Secur*., vol. 9, no. 1, pp. 67–75, 2017.

[11] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Advance DDOS detection and mitigation technique for securing cloud," *Int. J. Comput. Sci. Eng.*, vol. 16, no. 3, pp. 303–310, 2018.

[12] Z. Chen, C. K. Yeo, B. S. Lee, and C. T. Lau, "Power spectrum entropy based detection and mitigation of low-rate DoS attacks," *Comput. Networks*, vol. 136, pp. 80–94, May 2018.

[13] C. Modi and D. Patel, "A feasible approach to intrusion detection in virtual network layer of cloud computing," *Sādhanā*, vol. 43, no. 7, p. 114, Jul. 2018.

[14] C. Song, A. Pons, and K. Yen, "AA-HMM: An anti-adversarial hidden markov model for network-based intrusion detection," *Appl. Sci.*, vol. 8, no. 12, p. 2421, 2018.

[15] P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, "HIDS: A host based intrusion detection system for cloud computing environment," *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 3, pp. 567–576, Jun. 2018.

[16] C. Wang, H. Yao, and Z. Liu, "An efficient DDoS detection based on SU-Genetic feature selection," *Cluster Comput*., pp. 1–11, Mar. 2018.

[17] C. Boufenar, M. Batouche, and M. Schoenauer, "An artificial immune system for offline isolated handwritten arabic character recognition," *Evol. Syst*., vol. 9, no. 1, pp. 25–41, Mar. 2018.

[18] S. Forrest, B. Javornik, R. E. Smith, and A. S. Perelson, "Using genetic algorithms to explore pattern recognition in the immune system," *Evol. Comput*., vol. 1, no. 3, pp. 191–211, 1993.

[19] E. H. Spafford, "Computer viruses as artificial life," *Artif. Life*, vol. 1, no. 3, pp. 249–265, 1994.

[20] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection - a review," *Nat. Comput.*, 2007.

[21] R. Hightower, S. Forrest, and A. S. Perelson, "The Baldwin effect in the immune system: Learning by somatic hypermutation," in *Adaptive Individuals in Evolving Populations: Models and Algorithms*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 1996.

[22] N. Xu, Y. Ding, L. Ren, and K. Hao, "Degeneration recognizing clonal selection algorithm for multimodal optimization," *IEEE Trans. Cybern*., vol. 48, no. 3, pp. 848–861, Mar. 2018.

[23] R. Zhang and X. Xiao, "Study of danger-theory-based intrusion detection technology in virtual machines of cloud computing environment," *J. Inf. Process. Syst.*, vol. 14, no. 1, Feb. 2018.

[24] W. Wang, L. Ren, L. Chen, and Y. Ding, "Intrusion detection and security calculation in industrial cloud storage based on an improved dynamic immune algorithm," *Information Sciences*, July 2018.

[25] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection," *ICARIS*, vol. 3627, pp. 153–167, 2005.

[26] F. Gu, J. Greensmith, and U. Aickelin, "Integrating real-time analysis with the dendritic cell algorithm through segmentation," in *Proc. 11th Annual Conf. on Genetic and Evolutionary Computation*, 2009, pp. 1203–1210.

[27] S. Wang, X. Mu, P. Zhao, and D. Zhao, "An improved real-time dendritic cell algorithm for intrusion detection," in *Proc. Int. Conf. on Computer Science and Technology*, 2016, pp. 424–431.

[28] Z. C. Dagdia, "A scalable and distributed dendritic cell algorithm for big data classification," *Swarm Evol. Comput.*, Sep. 2018.

[29] A. Ahmad, M. N. Kama, O. M. Yusop, N. A. A. Bakar, and N. B. Idris, "Cloud denial of service detection by dendritic cell mechanism," presented at 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), April 28, 2018.

[30] R. Oates, G. Kendall, and J. M. Garibaldi, "Frequency analysis for dendritic cell population tuning," *Evol. Intell.*, vol. 1, no. 2, pp. 145–157, 2008.

Azuan Bin Ahmad is a Lecturer at Universiti Sains Islam Malaysia and Ph.D. holder in Cloud Security from Universiti Teknologi Malaysia (UTM). Previously he has Bsc. Hons. Computer Science (Information Security Assurance) in USIM, Malaysia and M.Sc. Computer Science (Information Security), UTM, Malaysia. His research work is on cloud security and malware research. His current research is on Cloud Intrusion Detection System.

Nazri Kama is an Associate Professor at Universiti Teknologi Malaysia (UTM) specializing in software engineering. He graduated in Bachelor in Management Information System from Universiti Teknologi Malaysia. Later, he obtained a Master's Degree from the same university in Real-time Software Engineering. In 2011, he received a Doctorate in Software Engineering from the University of Western Australia in Australia.

Azri Azmi is a Senior Lecturer at Universiti Teknologi Malaysia. His research interests' including the area of software Engineering, Software Testing, Software Traceability, Software Maintenance, Software Documentation, Software Requirement, Software Design.

Norbik Bashah is a Professor at Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia and is attached to Information Assurance and Security Research Group. His research interest is towards Network Security, Intrusion Detection systems, Soft computing etc. He is a Senior Member of IEEE and actively participates in Information Security research.