

BOTNET DETECTION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT: A SURVEY

M. Thangapandiyani¹, P. M. Rubesh Anand^{2*}^{1,2}Department of Electronics and Communication Engineering,
Hindustan Institute of Technology and Science, Chennai – 603103, India.^{2*}rubesh.anand@gmail.com

Abstract: Cloud computing defines a collection of processors, memory, storage space, applications, and other computing resources connected to the web that aims to provide services with minimal service provider interaction and minimal effort to the customers. The wide usage of cloud computing has made the individual cloud user to be least concerned about investing about any new infrastructure, training new personnel and purchasing or licensing new software. Due to the constant increase in the volume of information placed in the cloud, more security issues are needed to be addressed. Botnet is considered to be one of the major issues of cloud computing. Botnet contains a network of compromised nodes called bots and manages millions of computer resources, countless gigabytes of storage, and memory. Botnets do not focus on a specific business, instead, it spreads systematically by working through a list of IP addresses. The botmasters inject the malicious code to the computer devices and control the network of the infected group of nodes. Based on the activities of botnet, the attackers perform multiple criminal activities like, Distributed Denial of Service (DDoS), click fraud, phishing, spamming, sniffing traffic and spreading malware. The main challenge in cloud is to detect the botnets and to reduce its impact on the cloud network. In this paper, the different detection techniques based on user data and behavior of the distributed computing environment are studied and analyzed.

Keywords: Cloud Computing; Botmaster and Botclouds; Cloud Security; Intrusion Detection System; Distributed Denial of Service.

1. Introduction

Cloud computing technology is widely used by providers and consumers to store and access data via user interfaces like, web browsers. The advantages of cloud computing includes, significant cost reductions for the services provided, reduced hardware and maintenance cost, provided accessibility around the globe, and produced flexible and highly automated processes. These cloud computing benefits provide

customers with least concerns about the software up-gradations. The key services provided by the cloud environment are Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). In SaaS, the cloud providers host the complete application into the cloud and enable users to access them via internet.

The SaaS are hosted either directly onto the cloud infrastructure or hosted on the top of the IaaS and PaaS services. The payment for the SaaS applications are based on pay-per-use basis. In IaaS, the computational resources, storage and network facilities are provided as an internet based service to the customers. In PaaS, the users develop, deploy and supervise the tools, frameworks, platforms and other business services provided by the service providers.

Botnet is one of the major threats in cloud computing. It is the combination of two phrases, namely, Bot and Net. The phrase 'Bot' represents the Robot and the phrase 'Net' represents the Network. Botnet contains a network of infected computer devices, controlled by a human called botmaster or bot herder [1]. The presence of rich computing resources in cloud facilitates the botmasters to easily deploy or remove the Command and Control (C&C) server. The botmaster controls the infected devices remotely with the help of C&C servers. Once a node is infected with malicious scripts or codes, the infected node joins the botnet as instructed in the code and works for the botmasters without the knowledge of the user. The Botnet further proliferates itself to many devices and infects them. The attackers perform many criminal activities like DDoS, click fraud, phishing, spamming, sniffing traffic and spreading malware with the use of botnets. Based on the C&C channel, the botnets are classified into IRC, P2P botnet, HTTP botnet and hybrid botnet [2]. In order to identify the attacks caused by the botnet, the existing botnet detection techniques uses two main groups, namely, honeynets based detection technique and intrusion detection system [3].

This paper is further organized into five sections. Section II presents the different botnet detection techniques. Section III describes cloud botnet detection

techniques and analysis. Finally, the study is summarized and concluded in Section IV.

2. Botnet Detection Methods

The existing botnet detection techniques use two different methodologies to identify the attacks caused by the botnet, namely, honeynet based detection technique and intrusion detection system [4]. Once the botnet is detected, the threat impact reducing techniques such as proactive defense techniques and reactive defense techniques [5] are used to cure infections caused by the botnet. It is important to detect the botnets at their initial stages and prevent the attacks caused by them to protect the cloud network. As shown in Fig.1, the classification of the botnet detection techniques includes two main groups, namely, classification based on behavior and classification based on user data [6].

A. Classification based on behavior

The behavior of the botnet in the network devices and the analysis on their comportment aids in predicting their nature of attack on the network. The monitoring of such data leads to the classification based on behavior in two types, namely, active analysis and passive analysis.

1) Active Analysis

The active analysis detects the possible malwares and deactivates them. The botmaster either directly or indirectly knows the detection activity. Honeypot and

Honeynets are the common active analysis methods used for the botnet detection.

(i) **Honeypot:** Honeypots are vulnerabilities that are intentionally introduced to detect the intrusions and attacks in the cloud environment. Based on the emulation capacity, the honeypot is classified into two types, namely, high-interaction and low interaction. Almost all features of the real operating system are simulated in the high interaction honeypot. It provides response only to the known ports and protocols. The low interaction honeypot simulates only the key features of the real operating system. High interaction honeypot allows the attackers to gain full control of the operating system, whereas the low interaction honeypot restricts the attackers from gaining full control of the operating system due to the limited availability of features. Honeypot carries information, such as, signature of bots for content-based detection, information of the botnet C&C mechanisms and servers, unknown security holes that enable bots to penetrate the network, tools and techniques that the attackers use and the motivation of the attackers [7]. Nepenthe is a low-interaction honeypot [8] that focuses on the vulnerabilities of the malware binaries. The honeypot based botnet detection generates a report regarding the detected botnet to provide a better understanding about the consequences of the botnet [9]. Though the honeypots provide a better knowledge regarding the botnet characteristics and technology, the infections caused by botnets are not detected every time.

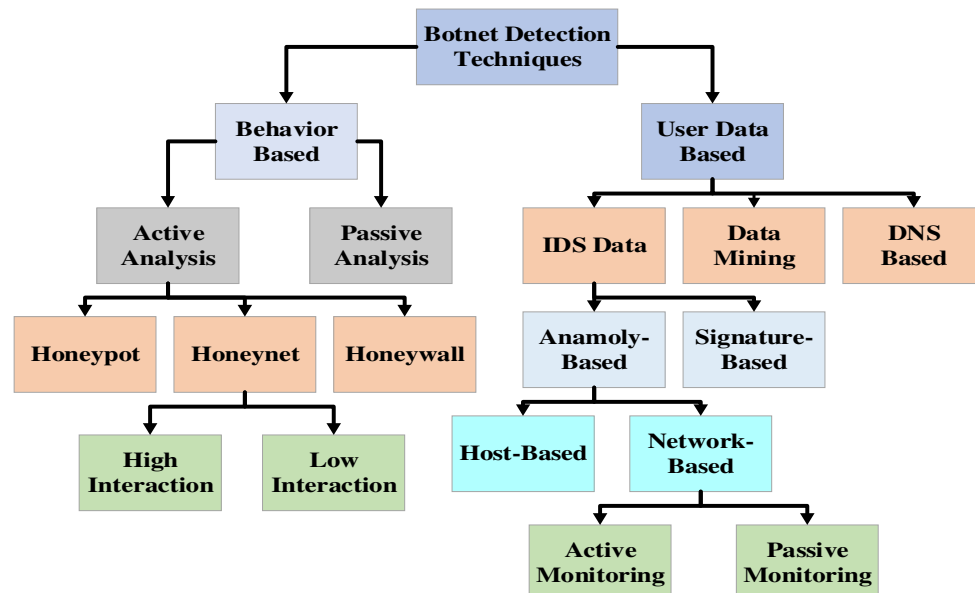


Figure 1. Categorization of Botnet detection techniques.

(ii) **Honeynets:** In the cloud network, different sizes of honeypots are combined to form a honeynet. Critical aspects of honeynet includes, limited scalability, unable to detect internet attacks, able to track only the malicious activities when interacting with it, challenges in discovering the infected systems, and systems that are affected by the implementation of honeybots are not controlled. Moreover, only the infected machines that are anticipated are reported.

(iii) **Honeywall:** The honeywall is the point of entry and exit for all the honeypot's network traffic. All the network traffic that enters and leaves the honeynet or honeypot system are controlled and analyzed by the honeywall. The collected network traffic assists the honeywall in their analysis procedure. The IP-address of C&C server, port address, authentication password, channel name of the connecting botnet are determined through the data capturing capability of the honeywall.

2) *Passive Analysis*

Passive analysis monitors the traffic created by the botnet without corrupting or changing the message. It mainly analyzes the secondary effects caused by the botnet traffic. The advantage of the passive analysis method is that the botmasters are unable to perceive detection activity. The passive analysis methods are very complex to be deployed in the cloud environment. Table 1 summarizes the active and passive botnet detection techniques with their merits and demerits.

B. *Classification based on user data*

The botnet behavior based analysis is an expensive task to deploy a dedicated honeypot or honeynet infrastructure for analysis and detection of botnets. But, the analysis based on the traffic and user related data collected from the client system helps in a less expensive way of detecting botnet related attacks. The classification based on the user data is of two kinds, namely, analysis based on Intrusion Detection System (IDS) data and Domain Name System (DNS) based detection technique.

Table 1. Comparison of Active and Passive Botnet Detection Techniques

Detection Technique	Botnet Detection	Attack created by the botnet	Protocol/ Channel used by the C&C	Techniques and its merits	Demerits	References
Active analysis	IRC	DDoS	IRC & P2P protocols	- Detects and identifies the root cause of the DDoS attack - Bots are tracked faster - Control network of the botnet can be shut down easily	- Sufficient information about the botnets are not gathered - The honeypots to capture the malware are not adaptable	[24], [25]
	Agobot DSNXbot	Change the C&C server, Spam	Does not rely on any specific protocol	Distinguishes the malicious bots from the harmless programs	Detection process to be updated regularly due to high number of variants in the bot	[7],[19],[26]
	Evilbot	Flooding attacks				[24],[2]
	G-SySbot Sdbot	Create spy	Generic approach is utilized	- Characterizes the remote control behavior of the bots - Content-based and substring-based	- Existing bot detection systems and honeypot are not secure and robust - Response	[15],[27]
	Spybot Win32 bots	Kill processes DDoS Floods				[22]

932

botnet controllers	collects the
• Detects	traffic
botnets that use	information
encrypted	from the
communication	selected traffic
	links

3) Analysis based on IDS data

The Intrusion Detection System is a reliable form of security monitoring system that collects the data and analyzes them for any malicious activities. Analysis based on the data from Intrusion Detection System is performed in two ways, namely, Anomaly based IDS and Signature based IDS.

i) Anomaly based IDS: The active anomaly based IDS compares the input data collected through IDS with the predicted behavior of the system. When an abnormal traffic behavior is found, the behavior based system detects the unknown botnet [10], [11]. The anomaly based system is categorized into two types, namely, host based, and network based detection. The host based detection focuses on the internals of the computer system whereas, network based detection identifies the botnets by observing the network traffic and comparing with the traffic statistics. The network based detection is further divided into two categories, namely, active monitoring and passive monitoring.

a) Host-based technique - The host based technique mainly observes and examines the internals of the host's machine than analyzing the external interfaces traffic data. In [12], a BotSwat is proposed to discover the programs that receive the network traffic from an unreliable external source. It also creates a significant amount of false positives in finding the potential remote control behavior of the bots.

b) Network-Based Technique - In this detection strategy, the entire network [13] traffic is monitored to detect the botnets. The network based technique is classified into active monitoring and passive monitoring techniques.

- **Active Monitoring** - The reaction of the network is measured by injecting the test packets into the network, servers or application. This method introduces some additional traffic apart from the data traffic. The botprobe is an active monitoring technique that is used for the botnet detection [14]. The botprobe injects well-crafted packets to the monitoring client while participating in the network session. In this technique, a deterministic command response pattern is provided by

a large portion of the botnet C&C channels and interactions.

- **Passive Monitoring** - The traffic is monitored periodically by passive monitoring techniques. The network traffic is not increased during the inspection of the network through passive monitoring but the detection of the botnets is a time consuming process. Many approaches combine TCP-based anomaly detection with IRC tokenization and IRC message statistics to detect the botnets. The network based anomaly detection is used to identify the botnet C&C channels in the Local Area Network [14]. Multiple correlation analysis algorithms are used to detect spatial-temporal correlation in the network. The anomaly mechanism monitors the group activities in the DNS traffic. The method of differentiating the valid DNS queries from the botnet DNS queries is found to be efficient than the other approaches [15]. In [16], the botnet traffic is detected by using the network based approach. The detection of the botnet traffic is composed of two steps. Initially the IRC flows are separated, then the botnet C&C traffic is discovered from the normal IRC flows. An effective flow based botnet traffic detection is performed by mining the multiple log files. The botnet traffic detection method uses multiple log correlation along with C&C traffic detection. The entire flow is categorized to identify the botnet C&C traffic [17]. In [18], the IRC based botnets are detected using the machine learning techniques. Initially, the IRC and the non IRC traffics are separated, then among the IRC traffics, the botnet IRC traffic and the real IRC traffic are distinguished.

ii) Signature based IDS: The signature based IDS performs a matching process between the new malicious traffic containing payload data and the knowledge base that has the signatures of known attacks. When there is a match between the acquired traffic information and the knowledge base, the signature based IDS gives an alarm. In [19], a popular signature based botnet detection technique, namely, Rishi is used to match the nick name patterns of the IRC bots. Passive traffic monitoring is used for analyzing the network for vulnerable IRC nicknames, IRC servers and uncommon server ports. An n-gram analysis and a scoring system is used to detect the bots

that use the uncommon communication channel. These channels are not detected by the traditional botnet detection techniques. The encrypted communication and the non-IRC bots are not detected by the Rishi. The signature based IDS are highly accurate. The demerits of this analysis is that the knowledge base should have up-to-date signatures and payload data has to be transformed and stored with the signature.

4) DNS based detection technique

The DNS based detection is used to detect the DNS traffic and its abnormalities. The bots implement the DNS queries to locate the DDNS (Dynamic DNS) provider that has hosted the C&C server. The DNS based detection technique is popular and easy for botnet detection, but the advanced botnets are difficult to be detected. If a simple botnet is created and the flow of information among the bots and the C&C server is analyzed. The botnet is detected using the DNS query patterns generated by the botnet [19].

5) Data Mining Detection Techniques

Data mining based botnet detection technique is used for the purpose of optimizing the collected user data. The network log file contains the complete data pertaining towards the network activity and the data mining detection takes the necessary data for analysis. Correlation, classification, clustering, statistical analysis and aggregation are the commonly used data mining techniques for discovering essential data from the network log file [20]. The flow correlation algorithm compares the network flow objects based on some specified characteristics. The flow correlation algorithm is effective when the contents of the packets are not encrypted and applying one or more functions to the characteristic value of the inputs lead to the decision of whether the network flow is correlated or

not. The classification algorithms compare the input packets with the previous patterns and detects the botnets. The disadvantage of the classification algorithm is that it fails to detect new attacks. Based on the similarity metric and feature value, the clustering methods of the data mining technique clusters the data points. It divides the input dataset into clusters of identical features. The advantage of clustering algorithm is that a labeled dataset for training is not required as in the classification techniques. Aggregation methods of the data mining based detection techniques are used to discover a particular pattern from the large datasets. The association rule mining techniques identify the correlation between the different items occurred in the same event [21]. Table 2 summarizes the various user data based botnet detection techniques.

3. Botcloud Detection Techniques

The DDoS attack launched by the botcloud has the same effect as the DDoS attack launched by the traditional botnet [22]. The CSPs need to constantly monitor the DDoS attack so that the attack is easily detected and neutralized by the CSP. The spam attacks are eliminated by backlisting the range of IP addresses from where the spam is sent. But in certain cases, the blacklisting of large range of IP addresses also block the legitimate cloud users requesting for services. The techniques for botcloud detection in the cloud environment uses the combination of the existing traditional botnet detection methods. But, the policies adopted in VMs like, SLA and security provision makes the CSPs to work with cautious in implementing the botnet detection methods. As in certain cases, the legitimate behavior of the user in the virtual machines may be mistakenly considered as a malicious one [23].

Table 2. Comparison of Various User Data Based Botnet Detection Techniques

Detecti on Techni que	Botnet Detection	Attack created by the botnet	Protocol/ Channel used by the C&C	Techniques and its advantages	Demerits	Referen ces
IDS based	- Suspici ous IRC nicknames - IRC serversunco mmon server ports	Creates high volume of SPAM	- IRC protocol - HTTP - Peer- to-Peer protocols	- Botnet infected machines within a network is detected - N-gram analysis detects the bots that use uncommon communication channel - Automatically	- Detects only the bots that has previous expressions. - Bots that use common name and real name are not detected	[3],[13], [24], [25], [27],[28],[29]

				informs the administrators about the attack	
DNS based	Botnet based spamming campaigns	Spam emails	Self-defined	• Leveraging the spam payload and spam server traffic, the spamming botnets are categorized. • Spam signature generation framework detects the botnet-based spam emails. • Low false positive rate • Low cost and low risk	• Protocol and structure dependent • Novel attacks and intrusions are not detected [24], [27]
	BotnetC&C servers	Multiple attacks due to compromised C&C server	Self-defined	• DDNS-based approach is used to identify the botnet C&C server in enterprise and access provider network • Anomalous DNS traffic is separated from the normal DNS traffic	• The increase in the number of bots • The detection method is very complex • Difficult to distinguish the DDNS from the other names in the enterprise and access provider networks [2], [7], [24]
	• All known botnets • Unknown botnets • False alarms	• Threshold attacks • Botnet Subgrouping • Synchronization minimization	IRC HTTP P2P	• DNS traffic is grouped • Botnet detection mechanism named BotGAD (Botnet Group Activity Detector) is used to detect the botnets from the large scale networks.	• Processing time is large • Large scale detection is not feasible [2], [15]
Data mining	HTTP botnet	• Click fraud • Identity theft • Information phishing • DDoS	HTTP protocol	• Combines the data mining techniques and timestamp. • Network filtering and separation process is performed. • Data mining algorithms automate the botnet detecting characteristics from large amount of data. • Easily applicable on network flow information • Effective as the flow information had internal patterns.	• Not focusing on the time duration. • Response time for larger datasets are also not considered. • Filtering process is not implemented for dynamic environment. • Flow parameters like response time, source port and destination port are not considered. [15], [24], [27]

Botcloud	Bot master	Trace back attacks	Cryptographic key mechanism	• Identification of cryptographic mechanism for network configuration • Design and implementation of key schemes on multiple clouds	• Huge volume of botnet traffic for high speed networks • Computational bottleneck problem	[31], [32]
	SAAS vulnerability	Security attack	Incident detection mechanism	• Secure service level agreements used for SAAS incident detection • Utilization of intrusion agents to specify incident detection	• More time consumption • Low feasibility in detection	[31], [32]

The analysis of detection depends upon the various characteristics of cloud based botnet namely, dynamic nature, skillful developers and flexibility. The variations in environment, more wide distribution and resilient botnets require advanced detection techniques and infrastructure. Various efficient detection approaches are available for large scale botnet environment. But, small scale botnet detection is a challenging issue for new environment. Auto updaters and self-refreshing web pages create the periodic pattern and increase the false positive rates. Botnets serving as phishing websites makes the botnet detection process a difficult one. The mobile botnets make the communication faster but, if the devices are out of range, the construction of the channel is very difficult. The active analysis techniques of botnet detection focus on the variety of botnets and they are less robust and secure when compared to the other detection techniques. In this survey, it is found that compared to the existing IRC botnet, peer-to-peer botnet, HTTP botnet, and mobile botnets, the new variant of botcloud is the most vulnerable C&C channel based botnets in the distributed computing environment.

4. Conclusion

An overview on the recent botnet types, botnet detection techniques and botnet impact reducing techniques are presented in this paper. On comparing the different types of botnet, the IRC botnet has low latency communication and botmasters have a real control over the bots. Also, the bots are easily collapsed by shutting down the IRC. The peer-to-peer botnets exhibits more strong encryption, resistance to failure but they have a very high latency communication. The HTTP botnet hides their vulnerable activities through the HTTP protocol, but the entire botnet are collapsed by shutting down the web servers and the botmasters do not have a complete control over the bots. The mobile botnets make the communication faster but, if the devices are out of range the construction of the channel

is very difficult. The bot cloud is the major issue of the cloud computing environment. The active analysis techniques of the botnet detection focus on the variety of botnets and they are less robust and secure when compared to the other detection techniques. The signature based IDS identifies the bots from the previous attack signatures but these techniques are not helpful to identify any novel attacks. The DNS traffic is analyzed in the DNS based detection techniques. Through the process of shutting down the botmaster, C&C and by taking the bot profit, the infections created by the botnets are cured.

References

- [1] R. A. Rodriguez-Gomez, G. Macia-Fernandez, and P. Garcia-Teodoro, "Survey and taxonomy of botnet research through life-cycle," *ACM Computer Survey*, vol. 45, no. 4, 2013.
- [2] D. Seenivasan and K. Shanthi, "Categories of Botnet: A Survey," *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 8, no. 9, pp. 1689-1692, 2014.
- [3] H. Jiang and X. Shao, "Detecting P2P botnets by discovering flow dependency in C&C traffic," *Peer-to-Peer Networking Applications*, vol. 7, no. 4, pp. 320-331, 2014.
- [4] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha and K. Kim, "Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection," *IEEE Transactions on Cybernetics*, vol. 46, no. 8, pp. 1796-1806, Aug. 2016.
- [5] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed and S. A. Khayam, "A Taxonomy of Botnet Behavior, Detection, and Defense," *IEEE*

- Communications Surveys & Tutorials, vol. 16, no. 2, pp. 898-924, Second Quarter 2014.
- [6] C.-Y. Liu, C.-H. Peng, and I.-C. Lin, "A survey of botnet architecture and botnet detection techniques," *International Journal of Network Security*, vol. 16, no. 2, pp. 81-89, 2014.
- [7] W. Chen, P. Gong, L. Yu, and G. Yang, "An adaptive push-styled command and control mechanism in mobile botnets," *Wuhan University Journal of Natural Sciences*, vol. 18, no. 5, pp. 427-434, 2013.
- [8] M. Thangapandiyan and P. M. Rubesh Anand, "A secure and reputation based recommendation framework for cloud services," in *IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016, Chennai, India, 2016*, pp. 1-4.
- [9] T.-Z. Wang, H.-M. Wang, B. Liu, and P.-C. Shi, "Some critical problems of botnets," *Chinese Journal of Computers*, vol. 35, no. 6, 2012.
- [10] A. Feizollah, N. B. Anuar, R. Salleh, F. Amalina, R. R. Ma'arof, and S. Shamshirband, "A study of machine learning classifiers for anomaly-based mobile botnet detection," *Malaysian Journal of Computer Science*, vol. 26, no. 4, pp. 251-265, 2013.
- [11] J. Wang; I. C. Paschalidis, "Botnet Detection based on Anomaly and Community Detection," in *IEEE Transactions on Control of Network Systems*, no. 99, 2016.
- [12] E. Stinson and J. C. Mitchell, "Characterizing bots' remote control behavior," in *Botnet Detection*, Springer, 2008, pp. 45-64.
- [13] Y.-Z. Song, J.-T. He, B. Zhang, J.-J. Wang, and A.-B. Wang, "Detecting P2P botnet based on the role of flows," *Journal on Communications*, vol. 33, no. 1, pp. 262-269, 2012.
- [14] G. Gu, V. Yegneswaran, P. Porras, J. Stoll and W. Lee, "Active Botnet Probing to Identify Obscure Command and Control Channels," *Annual Computer Security Applications Conference*, Honolulu, HI, 2009, pp. 241-253.
- [15] H. Jiang, Y. Liu, and X. Shao, "BotCVD: Visual analysis of DNS traffic for botnet detection," *Advances in Information Sciences & Service Sciences*, vol. 4, no. 8, 2012.
- [16] M. Thangapandiyan and P. M. Rubesh Anand, "Robust charm: An efficient data hosting scheme for cloud data storage system," *Automatic Control and Computer Sciences*, vol. 51, no.4, pp. 240-247, 2017.
- [17] Z. Futai, Z. Siyu and R. Weixiong, "Hybrid detection and tracking of fast-flux botnet on domain name system traffic," in *China Communications*, vol. 10, no. 11, pp. 81-94, Nov. 2013.
- [18] R. S. Abdullah, N. A. Abu, M. A. Faizal, and Z. A. M. Noh, "Understanding the threats of botnets detection: A wide scale survey," *Research Journal of Information Technology*, vol. 6, no. 3, pp. 135-153, 2014.
- [19] W. Chen, S.-W. Zhou, and C.-Y. Yin, "Research on cloud-based traffic adaptive command and control method for mobile botnet," *Journal on Communications*, vol. 35, no. 11, pp. 32-38, 2014.
- [20] H.-L. Jiang, X.-L. Shao, and Y.-F. Li, "Online botnet detection algorithm using MapReduce," *Journal of Electronics & Information Technology*, vol. 35, no. 7, pp. 1732-1738, 2013.
- [21] K.-C. Lin, S.-Y. Chen, and J. C. Hung, "Botnet detection using support vector machines with artificial fish swarm algorithm," *Journal of Applied Mathematics*, vol. 2014, pp. 1-9, 2014. DOI:10.1155/2014/986428.
- [22] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242-2270, Fourthquarter 2015.
- [23] Y. Ji, Y. He, X. Jiang, J. Cao, and Q. Li, "Combating the evasion mechanisms of social bots," *Computers & Security*, vol. 58, pp. 230-249, 2016.
- [24] M. Eslahi, R. Salleh and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," in *IEEE International Conference on Control System, Computing and Engineering*, Penang, 2012, pp. 349-354.
- [25] W. Zhu and C. Lee, "Internet security protection for IRC-based botnet," in *IEEE 5th International Conference on Electronics Information and Emergency Communication*, Beijing, 2015, pp. 63-66.
- [26] J. Wang and I. C. Paschalidis, "Botnet detection using social graph analysis," in *52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, 2014, pp. 393-400.

- [27] P. Narang, C. Hota, and H. T. Sencar, "Noise-resistant mechanisms for the detection of stealthy peer-to-peer botnets," *Computer communications*, vol. 96, pp. 29-42, 2016.
- [28] Y. Song, "Detecting P2P botnet by analyzing macroscopic characteristics with fractal and information fusion," *China Communications*, vol. 12, no. 2, pp. 107-117, Feb. 2015.
- [29] M. Thangapandiyar and P. M. Rubesh Anand, "An efficient botnet detection system for P2P botnet," in *IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016, Chennai, India, 2016*, pp. 1217-1221.
- [30] J. Zhang, R. Perdisci, W. Lee, X. Luo and U. Sarfraz, "Building a Scalable System for Stealthy P2P-Botnet Detection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 27-38, Jan. 2014.
- [31] M. Torkashvan and H. Haghighi, "CBC2: A cloud-based botnet command and control," *Indian Journal of Science and Technology*, vol. 8, no. 22, pp. 1-15, 2015.
- [32] M. R. Memarian, M. Conti, and V. Leppänen, "EyeCloud: A BotCloud detection system," in *IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom 2015)*, Helsinki, pp. 1067-1072, 2015.

