Journal of Computer Science 10 (10): 2029-2036, 2014
ISSN: 1549-3636
© 2014 Science Publications
doi:10.3844/jcssp.2014.2029.2036 Published Online 10 (10) 2014 (http://www.thescipub.com/jcs.toc)

INTRUSION DETECTION SYSTEM IN SECURE SHELL TRAFFIC IN CLOUD ENVIRONMENT

**Mehdi Barati, Azizol Abdullah, NurIzura Udzir,
Mostafa Behzadi, Ramlan Mahmod and Norwati Mustapha**

Faculty of Computer Science and Information Technology, Serdang, Malaysia

Received 2014-04-12; Revised 2014-06-20; Accepted 2014-06-26

ABSTRACT

Due to growth of Cloud computing usage, the need to apply encrypted protocols to provide confidentiality and integrity of data increases dramatically. Attacker can take advantage of these protocols to hide the intrusion and evade detection. Many traditional attack detection techniques have been proposed to provide security in the networks but none of them can be implemented properly in encrypted networks. This study investigates a popular attack in Secure Shell (SSH), known as brute force attack and provides an efficient method to detect this attack. Brute force attack is launched by implementing a client-server SSH model in a private Cloud environment and the traffics regarding attack and normal are captured on the server. Then, representative features of traffic are extracted and used by the Multi-Layer Perceptron model of Artificial Neural Network to classify the attack and normal traffic. Results gained by this method show that the proposed model is successfully capable to detect this attack with high accuracy and low false alarm.

Keywords: Brute Force Attack, Intrusion Detection System, Cloud Environment, Encrypted Traffic, SSH Traffic, Machine Learning, ANN

1. INTRODUCTION

Cloud computing is one of the emerging technologies these days. It is an Internet-based technology to use dynamically scalable and virtualized resources. According to Mell and Grance (2011), Cloud computing is a kind of technology that provides convenient and on-demand access to shared resources through the Internet. This technology is growing significantly and becomes popular nowadays. Since the resources in Clouds are usually shared by users, the security of Cloud should be considered by the provider. Usually, services in the Cloud are provided through the Internet. Therefore, a major security concern in Cloud infrastructures is attack detection system. Vulnerabilities caused by virtualization and Internet in the Cloud attract many attackers to this technology. Some of these attacks affect the foundation of the Cloud technology including Denial of Service, backdoor attacks, attacks on Virtual Machine (VM) and malware attacks (Krishnan and Chatterjee, 2012; Modi *et al*., 2013). But some of these attacks focus on encrypted protocols itself and try to launch the attack in encrypted traffic. An Intrusion Detection System (IDS) is a system used to monitor and detect unauthorized activities into computer systems and networks (Ros *et al*., 2009). Many kinds of IDS in network have been proposed by researchers, however proposing more efficient IDS to detect attacks in encrypted traffic specifically in Cloud environment, is still one of the research interests.

Requirements regarding the Cloud architecture such as encrypting transferring traffic should be considered in designing IDS in Cloud. In a shared Cloud environment, unprotected traffic posed some security threats. Moreover, Cloud users in each layer of service need to be sure about their data integrity and privacy. The best method to provide data privacy and integrity is encrypting these traffics. Therefore, in a shared virtualized or Cloud environment, it is critical that traffic containing sensitive information are encrypted (Ponnuramu and Tamilselvan, 2012). Consequently, any proposed detection techniques for Cloud environment should be able to detect encrypted malicious traffic.

Corresponding Author: Mehdi Barati, Faculty of Computer Science and Information Technology, Serdang, Malaysia

Traditional IDS which emphasizes on using only Deep Packet Inspection (DPI) techniques are not efficient in encountering encrypted malicious traffic. One popular protocol in encrypting traffic is SSH which is used to provide a Secure Shell in a client-server model. It is susceptible in many kind of attacks, but one of the most significant attacks on SSH protocol is brute force attack (Mansfield-Devine, 2012). This kind of attack which is also known as Dictionary attack aims to log in to the SSH server by continuously guessing a large number of username and password combinations. Recently, some detection techniques have been proposed for this kind of attack in encrypted traffic but none of them is efficient enough in terms of accuracy and other requirements. Moreover, there is no any related research in Cloud environmet. One efficient method for detecting attack in encrypted environment is implementing Machine Learning (ML) techniques using flow-based features instead of packet-based features. Indeed, a flow is a sequence of packets between two nodes passing an observation point in the network during a certain time interval. In this study an efficient model using flow-based features for detecting brute force attacks in Cloud environment is proposed by getting the advantages of the Multi-Layer Perceptron (MLP) classifier. MLP isfeedforwardArtificial Neural Network model and Machine Learning technique to classify new instances using training dataset (Veselý and Brechlerová, 2004).

The rest of the paper is organized as follows: Section 2 provides a review of the proposed IDS in encrypted traffic and classified these systems based on the detection techniques. Our proposed method to detect brute force attack in SSH traffic is discussed in section 3. It also explains the data collection scenario, experimentation and the classifier used in this research. Sections 4 and 5 provide the results of the proposed method and the conclusion, respectively.

As the context of this research is Cloud environment, in this section we provide a short review of Cloud computing. Then, one security threat for SSH security protocol which is applied commonly in Cloud environment is discussed. Finally, some proposed detection methods for attack in encrypted traffic are reviewed in the current section.

1.1. Cloud Computing

The next generation of distributed computing, Cloud computing, has emerged as the evolution of grid, utility and high performance computing. The term ‘Cloud computing’ has been defined by many researchers and experts. It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Khorshed *et al*., 2012). Indeed, Cloud computing is a metaphor which refers to a set of characteristics such as resource sharing, multi-tenancy, virtualization, elasticity, pay-as-you-go and on-demand services. Virtualization is a key element in the infrastructure of Cloud computing that facilitates resource sharing for cloud vendors among users by running several VMs on one physical machine. The ability to perform intrusion detection in the Cloud is heavily dependent on the model of Cloud computing that is being used. According to Albaroodi *et al*. (2014), Services provided in Cloud environment can be grouped into three main categories, including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Despite the advantages of Cloud computing, several issues are relevant to this new field of technology. Among these challenges, security is the most significant challenge which can cause a serious threat to users’ assets (Khorshed *et al*., 2012). Due to the high usage of encryption in Cloud environment, security issues of encrypted traffic are concerned in this research.

1.2. Brute Force Attack in SSH

Secure Shell (SSH) protocol aims to provide integrity and confidentiality of data between client and server in an insecure network. SSH runs on top of TCP protocol and is usually implemented to provide a secure command shell or file copy. In addition to encryption, this protocol also applies encapsulation to provide a tunnelling service. SSH establishes the secure tunnel by using a client-server model in which server listens to port 22 for any session request by client on this port (Dusi *et al*., 2009).

According to Mansfield-Devine (2012), malicious SSH login attempts known as brute force attack can be launched by an attacker. It also was named as Dictionary attack and aims to log in to the scanned hosts to gain fraudulent access by continuously guessing a large number of username and password combinations. In some cases, distributed brute force attack is launched which is very stealthy in comparison with a simple brute force. This kind of attack is launched by a group of malicious hosts, such as botnets (**Fig. 1**).

1.3. IDS in Encrypted Traffic

The first step to design appropriate IDS is to understand the current technology of IDS. According to Patel *et al.* (2012), on functional layer IDSs can be classified based on two classifications.

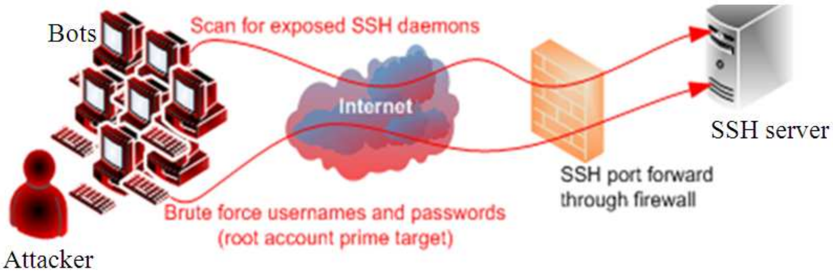
Bots
Scan for exposed SSH daemons
Internet
SSH server
SSH port forward through firewall
Brute force usernames and passwords (root account prime target)
Attacker

Fig.1. SSH brute force attack

One classification is based on the monitored environment, which divides IDSs into two groups including Host-based IDS (HIDPS) and Network-based IDS (NIDPS). Due to the inability of decryption by NIDS, attack in encrypted traffic cannot be detected by this type of IDS. In the other classification in the functional layer, IDS are classified into three classes of anomaly, misuse and hybrid model based on detection methods. The most used techniques of these methods are Machine Learning (ML). In ML-based technique the system uses learning, testing and improving its performance over time. ML methods are used in the current research for classifying attack and normal traffic in encrypted traffic. In encrypted traffic classification field, data mining methods were also used to classify traffic based on encryption protocol. Cao *et al*. (2013) presented a comprehensive review of studies which have used ML as well as other techniques to classify encrypted traffic. Since our research investigates on IDS, a short review of three classes of the proposed IDS for encrypted traffic will be presented inthe next section. These three classes include encryption protocol-based approach, modification-based approach and traffic analysis-based approach. In encryption protocol-based IDS, the misuse of the encryption protocols is detected. Some IDSs including those that have been proposed by Sperotto *et al*. (2009), Fadlullah *et al*. (2010) and Hellemons and Hendriks (2012), presented techniques to detect this kind of attack against encrypted protocols. Although their method is suitable for detecting any attack on encrypted protocol itself, it is not able to detect malicious activities hidden inside the encrypted tunnel. In modification-based IDS for encrypted traffic, the network infrastructure is modified to detect the intrusion. The encrypted traffic is duplicated and sent to both receiver and IDS using an additional encryption layer to preserve the confidentiality. Li and Zhang (2009; Goh *et al*., 2010) proposed IDS by integrating a NIDS into an encrypted network. This method is not possible to be implemented in all environments due to its inability of decrypting traffic in some scenarios. A good illustration of these scenarios can be an IDS implemented in hypervisor layer in Cloud environment which is not authorized to decrypt user's traffic. Users do not intend for their traffic to be identified and decrypted by the Cloud provider. On the other hand, it is expected that the Cloud provider desires to detect any incoming and outgoing attack in the Cloud. Therefore, some detection techniques should be proposed without decrypting the traffic. The last approach is analysing the encrypted traffic statistically to gain information from frequently observed patterns. The key idea is that packet and flow-based information are enough to infer the nature of the application protocol that generated those packets. There are some studies that have focused on using data mining to classify encrypted traffic. SSH and Skype traffic classification using ML method was proposed by Alshammari and Zincir-Heywood (2009). In addition, Barati *et al*. (2013) proposed a feature selection IDS in Encrypted Traffic Using Genetic Algorithm (GA). SSL traffic classification in Google traffic was proposed by Fu *et al*. (2013) using C4.5 algorithm. Furthermore, considering harmonic mean as distance metric in clustering approach was implemented by Zhang *et al*. (2013) to classify real-world encrypted traffic. However, our research tries to move one more step forward and detect attack inside encrypted traffic. In detecting attack in encrypted traffic, there are some researches that are briefly discussed in this section. Attacks were detected without decryption using the intrusion signatures by Foroushani *et al*. (2008) for SSH encryption and anomaly detection by Augustin and Balaz (2011) using data mining for SSL encryption. Their results demonstrated detection with undeniable false alarm. Dusi *et al*. (2009) a technique for blocking unwanted tunnelled traffic known as tunnel hunter proposed by characterizing legitimate uses of application-layer protocols. Their method was capable to detect this traffic by fingerprinting allowed protocols even in encrypted tunnelled protocol including SSH. Results demonstrated that tunnel hunter was able to detect legitimate tunnels with high accuracy except P2P tunnelled traffic. Due to high false alarm rate, their systems are not efficient enough for a production environment. Moreover none of proposed studies have implemented their methods in Cloud environment. As mentionedabove, usually in virtual machines in Cloud environment, data is transferred in an encrypted tunnel in order to provide confidentiality and integrity of data. Due tothe increasing popularity and importance of Cloud, in this research a method using artificial neural network as classifier is proposed to detect brute force attack on encrypted and tunnelled traffic in private Cloud environment.

2. MATERIALS AND METHODS

This section focuses on the proposed method for detecting brute force attack in Cloud environment. Initially, in the collection step one model was implemented in a real Cloud environment and the traffic regarding the attack was collected. Then our classifier was employed to identify attack and non-attack traffic.

2.1. Dataset

The appropriate collection of traffic containing ground truth information is one of the basic aspects in the classification process. In this step, a brute force attack was launched by implementing a client-server SSH model in a private Cloud environment. This private Cloud implemented in the Security Lab at the Universiti Putra Malaysia, Malaysia. Our assumption is that we implement only brute force attack and the traffic between the client and server is transferred only by SSH protocol. Moreover, we assume that the attacker is aware about some information regarding the target including the IP address and network details. **Figure 2** shows the structure of our model to implement SSH brute force attack in Cloud. When the attack is launched in the server side, encrypted traffic is captured. This traffic together with normal traffic collected in normal state of our model areused in the training step. Indeed, captured traffic are authentication requests to the SSH server including exact time, account and password used for the authentication request and other information for every packet in that specific time. Both attack traffic and non-attack traffics are converted to flow by grouping-related packets. Total 6283 number of flows were selected as a sample to be applied in the classification phase. A flow is a sequence of packets from a source to a destination passing an observation point in the network during a certain time interval.

2.2. Classifier

Machine Learning (ML) is an application of artificial intelligence that uses algorithms to provide learning using input data. It is used to efficiently identify patterns in large amounts of information that can be difficult to be done by very skilled human. A ML algorithm receives multiple instances and attributes in the training phase to form a model. This model is used to identify new instances in the testing phase.There are many prominent ML algorithms used in classification problems. Some of these algorithms are techniques inspired from natural phenomena and using adaptive learning over a training dataset (Veselý and Brechlerová, 2004). In this research a ML technique which is Artificial Neural Network (ANN) is implemented to classify attack and non-attack traffics. One of the most significant advantages of ANN is that a few parameters of this technique need to be optimized in the training phase. In addition, itis inspired by the human brain which contains billions of neurons. In a brain, information can be processed by exchanging electrical pulses between these neurons. These neurons are linked to each input by synaptic weights and generate output on the other side. ANN attempts to apply this concept in the field of computer systems to solve classification problems. Each ANN model has three layers as input layer, hidden layer and output layer. There are one or more neurons in each layer and layers are connected to each other using a network of neurons. Three layers of ANN are illustrated in **Fig. 3**.

Multi-Layer Perceptron (MLP) is a class of ANN technique that maps a set of input into a set of suitable output. Indeed, it is the best known and most widely used class of ANN (Veselý and Brechlerová, 2004). As mentioned above, some important flow-based features were extracted in aggregation of packets to generate flows and feature extraction step. In order to improve the detection speed and decrease computational cost of our method, redundant or irrelevant features are omitted and the best features were selected in the feature selection step. Moreover, to improve the robustness of our method, port and IP-based features were deleted. A Wrapper method, which uses a predictive model to scorefeature subsets, was used in our research. In the Wrapper method, the model is trained foreach new subset and then tested on the dataset. It usually provides the best performingfeature set and consequently best results.Therefore, to implement ANN in IDS context, selected features are imported to the input layer and forwarded to the hidden layer. After running the model, the classification results (attack or non-attack) arepresented in the output layer. MLP with nonlinear activation function is applied in this research to detect brute force attack in SSH encrypted traffic. The activation functions used in the current research is Sigmoid and described by the following Equation 1:

$$y\left(v_i\right)=\left(1+e^{-v_i}\right)^{-1} \tag{1}$$

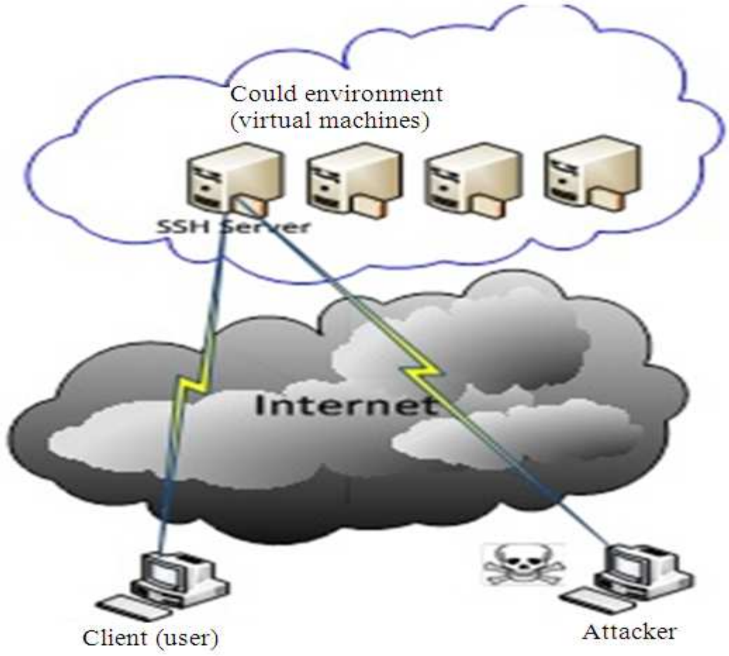

Fig. 2. Data collection design

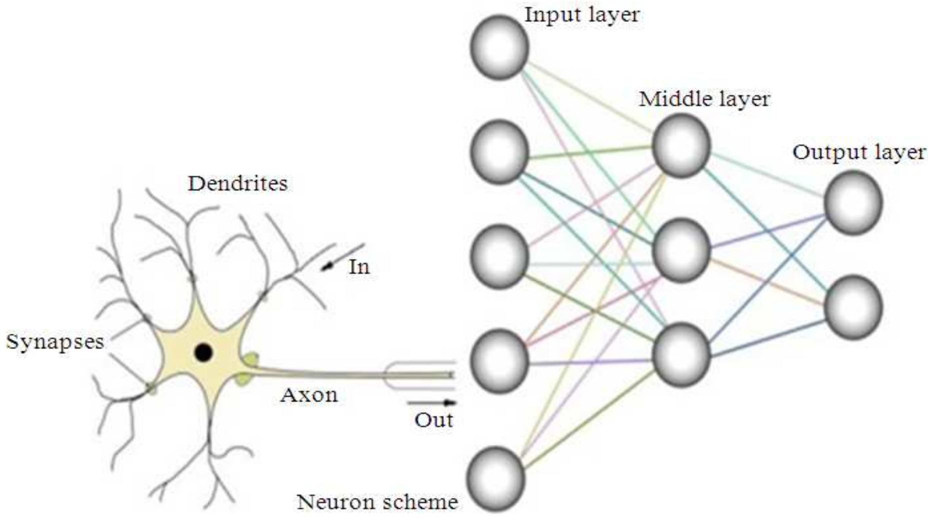

Fig. 3. Three layers in ANN

Here $y(v_i)$ is the output of the ith node (neuron) and v_i is the weighted sum of the input synapses.

2.3. Experimentation

The WEKA, an open-source Java machine learning application, is utilized in this research to apply the MLP algorithm. To ensure that one part of the dataset is not reused for training or testing, 10 folds cross validation technique was performed in our experiment. In this technique, the dataset is separated into 10 equal-size folds. So, in each round, one of the subsets is selected for testing and the rest are used for training. This routine is applied for each fold and returns the last result by averaging all folds results.

3. RESULTS AND DISCUSSION

The proposed method was evaluated by some metrics including Precision, Recall, F-measure, Receiver Operating Characteristic (ROC) area and True Positive and False Positive parameters. Precision is the fraction of retrieved instances that are relevant although Recall is the fraction of relevant instances that are retrieved. F-Measureconsiders both Precision and Recall to compute the score. Indeed, it is considered as weighted average of these two metrics. ROC curve is created by plotting True Positive Rate (TPR) versus False Positive Rate (FPR). Area Under Curve (AUC) is also used to evaluate classifier efficiency. All the mentioned metrics reach their best values at 1 and worst value at zero. These metrics can be calculated using the following Equation 2 to 4:

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F\_measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (4)$$

Our result demonstratesexcellent values in terms of these metrics. According to the resultin **Table 1**, the correctly classified instancesare quite high, i.e., around 94%. It also showed that the mean absolute error is deniable amount around 0.07%. It means that the attack traffic is accurately and precisely identified among the encrypted traffic. Moreover, the average Precision, Recall, F-measure and ROC area values are 0.943, 0.942, 0.943 and 0.978 respectively, which are promising results (**Table 2 and 3**). The proposed model also produced a low False Positive Rate (FPR), around 1.6%. In addition to the promising results, it can be noted that our model is applied in a private Cloud environment which can contribute the security models for this area.

As discussed, ROC curve is created by plotting the fraction of True Positives out of the positives (TPR) versus the fraction of false positives out of the negatives (FPR) at different threshold values. It is applied in the training process to find the best trained model as well as testing process to provide the performance of the classification. Area Under Curve (AUC) is also often used in evaluation of classification and express probability that classifier rank a randomly chosen positive instance higher than a randomly chosen negative one.

Table 1. Error rates

Parameter	Value (%)
Correctly classified instances	94.2066
Mean absolute error	0.0684

Table 2. Overview of result

TP rate	FP rate	Precision	Class
0.81	0.037	0.777	Non-attack
0.963	0.190	0.970	Attack
0.942	0.169	0.943	Average

Table 3. Overview of results

Recall	F_measure	ROC Area	Class
0.81	0.793	0.978	Non-attack
0.963	0.966	0.978	Attack
0.942	0.943	0.978	Average

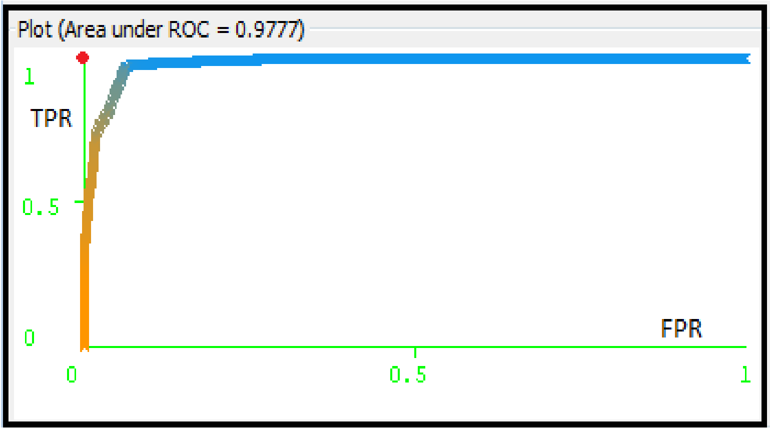

Fig. 4. ROC curve for classifier

As demonstrated in **Fig. 4**, the red point is the most optimum result in the classification which produces the highest TPR and lowest FPR. The ROC curve of our classification is very near to this point which verifies the efficiency of our system. By comparing our result with other studies in attack detection in encrypted traffic it can be revealed that none of the previous studies has reached such accurate results in terms of accuracy, precision and recall. According to our results, False Positive is very close to zero and can be denied by the system.

4. CONCLUSION

Due to the growth of Cloud computing usage, applying encrypted protocols to provide confidentiality and integrity of data is increasing dramatically. Beside the advantages of this method, some challenging issues appear in the presence of the growing trend of encrypted traffic usage. One vital issue in this context is the fact that malicious element hidden in encrypted or tunnelled traffic can evade the detection techniques. This research emphasizes on one detection technique in encrypted traffic and provides a review of recent proposed IDSs in this context. For a comprehensive development of IDS in encrypted traffic for productive environments, false alarms should be minimized. In this study, the Multi-Layer Perceptron (MLP) algorithm for attack detection in encrypted traffic is implemented. MLP is one efficient method of Artificial Neural Network techniques and produces excellent results. The presented results have proven this statement. It can distinguish brute force attack traffic from non-attack traffic efficiently in terms of detection rate and false alarms. Utilization of other machine learning methods to get a better result from our dataset is considered as the future work of this study.

5. REFERENCES

Albaroodi, H., S. Manickam and P. Singh, 2014. Critical review of openstack security: issues and weakness. J. Comput. Sci. 10: 23-33. DOI: 10.3844/jcssp.2014.23.33

Alshammari, R. and A.N. Zincir-Heywood, 2009. Machine learning based encrypted traffic classification: Identifying SSH and skype. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, Jul. 8-10, IEEE Xplore Press, Ottawa, ON., pp: 1-8. DOI: 10.1109/CICYBS.2009.4925105

Augustin, M. and A. Balaz, 2011. Intrusion detection with early recognition of encrypted application. 15th proceedings of the IEEE International Conference on Intelligent Engineering Systems, Jun. 23-25, IEEE Xplore Press, Poprad, pp: 245-247. DOI: 10.1109/INES.2011.5954752

Barati, M., A. Abdullah, R. Mahmod, N. Mustapha and N.I. Udzir, 2013. Feature selection for IDS in encrypted traffic using genetic algorithm. Proceedings of the 4th International Conference on Computing and Informatics, (ICCI’ 13), pp: 279-285.

Cao, Z., S. Cao, G. Xiong and L. Guo, 2013. Progress in study of encrypted traffic classification. Proceedings of the International Conference on Trustworthy Computing and Services, May 28-Jun. 2, Springer Berlin Heidelberg, Beijing, China, pp: 78-86. DOI: 10.1007/978-3-642-35795-4_10

Dusi, M., M. Crotti, F. Gringoli and L. Salgarelli, 2009. Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting. Comput. Net., 53: 81-97. DOI: 10.1016/j.comnet.2008.09.010

Fadlullah, Z.M.Z., T. Taleb, S. Member and A.V. Vasilakos, 2010. DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACM Trans., 18: 1234-1247.

Foroushani, V.A., F. Adibnia and E. Hojati, 2008. Intrusion detection in encrypted accesses with SSH protocol to network public servers. International Conference on Computer and Communication Engineering, May 13-15, IEEE Xplore Press, Kuala Lumpur, pp: 314-318. DOI: 10.1109/ICCCE.2008.4580619

Fu, P., L. Guo, G. Xiong and J. Meng, 2013. Classification research on SSL encrypted application. Proceedings of the International Conference on Trustworthy Computing and Services, May 28-Jun. 2, Springer Berlin Heidelberg, Beijing, China, pp: 404-411. DOI: 10.1007/978-3-642-35795-4_51

Goh, V., J. Zimmermann and M. Looi, 2010. Experimenting with an intrusion detection system for encrypted networks. Int. J. Bus., 5: 172-191.

Hellemons, L. and L. Hendriks, 2012. SSHCure: A flow-based SSH intrusion detection system. Proceedings of the 6th IFIP WG 6.6 International Autonomous Infrastructure, Management and Security Conference on Dependable Networks and Services, Springer Berlin Heidelberg, Luxembourg, Jun. 4-8, pp: 86-97. DOI: 10.1007/978-3-642-30633-4_11

Khorshed, M.T., A.B.M.S. Ali and S.A. Wasimi, 2012. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst., 28: 833-851. DOI: 10.1016/j.future.2012.01.006

Krishnan, D. and M. Chatterjee, 2012. An adaptive distributed intrusion detection system for cloud computing framework. Proceedings of the International Conference on Recent Trends in Computer Networks and Distributed Systems Security, Oct. 11-12, Springer Berlin Heidelberg, Trivandrum, India, pp: 466-473. DOI: 10.1007/978-3-642-34135-9_45

Li, L. and Z. Zhang, 2009. An intrusion detection model orienting towards encrypted conversation. Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology, Aug. 8-11, IEEE Xplore Press, Beijing, pp: 541-545. DOI: 10.1109/ICCSIT.2009.5234889

Mansfield-Devine, S., 2012. Interview: Tatu Ylönen, SSH communications security. Comput. Fraud Security, 2012: 13-16. DOI: 10.1016/S1361-3723(12)70042-8

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing: Recommendations of the national institute of standarts and technology. National Institute of Standards and Technology US.

Modi, C., D. Patel, B. Borisaniya, H. Patel and A. Patel *et al*., 2013. A survey of intrusion detection techniques in Cloud. J. Netw. Comput. Applic., 36: 42-57. DOI: 10.1016/j.jnca.2012.05.003

Patel, A., M. Taghavi, K. Bakhtiyari, J.C. Júnior and J. Celestino Júnior, 2012. An intrusion detection and prevention system in cloud computing: A systematic review. J. Netw. Comput. Applic., 36: 25-41. DOI: 10.1016/j.jnca.2012.08.007

Ponnuramu, V. and L. Tamilselvan, 2012. Data integrity proof and secure computation in Cloud computing. J. Comput. Sci., 8: 1987-1995. DOI: 10.3844/jcssp.2012.1987.1995

Ros, S., F. Cheng and C. Meinel, 2009. Intrusion detection in the cloud. Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec, 12-14, IEEE Xplore Press, Chengdu, pp: 729-734. DOI: 10.1109/DASC.2009.94

Sperotto, A., R. Sadre, Boer, P. De and A. Pras, 2009. Hidden markov model modeling of SSH brute-force attacks. Proceedings of the 20th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management: Integrated Management of Systems, Services, Processes and People in IT, Oct. 27-28, Springer Berlin Heidelberg, Italy, pp: 164-176. DOI: 10.1007/978-3-642-04989-7_13

Veselý, A. and D. Brechlerová, 2004. Neural networks in intrusion detection systems. Agric. Econ., 50: 35-39.

Zhang, M., H. Zhang, B. Zhang and G. Lu, 2013. Encrypted traffic classification based on an improved clustering algorithm. Proceedings of the International Conference on Trustworthy Computing and Services, May 28-Jun. 2, Springer Berlin Heidelberg, Beijing, China, pp: 124-131. DOI: 10.1007/978-3-642-35795-4_16