A Survey on Cloud Attack Detection using Machine Learning Techniques

Gavini Sreelatha
Research Scholar
Lincoln University College, Kuala Lampur, Malaysia

A. Vinaya Babu, PhD
Professor, Stanley College of Engineering and Technology for Women, India

Divya Midhunchakkarvarthy, PhD
Associate Professor, Lincoln University College, Kaula Lampur, Malaysia

ABSTRACT
Cloud concepts such as resource sharing, outsourcing, and multi-tenancy create significant challenges to the security community. Also, trusted third party and web technologies based cloud service provisioning arises new security threats in the cloud environment. Cloud security has become a vital research area with new security models, protocols, and policies in recent years. Despite the fact, the existing cloud security research still faces the shortcomings in improving the detection accuracy and detecting the new or unknown attacks in the cloud. To address the constraints above, many security researchers have focused on developing cloud security models with the assistance of the machine learning methods. Machine learning techniques play a significant role in automatically discovering the potential difference between legitimate and malicious data with high accuracy. The deep learning is a branch of machine learning that provides remarkable performance in cloud security issues. This survey provides a comprehensive study of cloud security concerns, traditional security measures, and machine learning-based security solutions in the cloud environment. Initially, it identifies cloud vulnerabilities and presents state-of-the-art methods to control security threats, weaknesses, and attacks. This work also reviews the security solutions developed by machine learning and deep learning techniques for the cloud environment.

Keywords
Cloud Computing, Cloud Security, Security Threats, Vulnerabilities, Attacks, Machine Learning, and Deep Learning.

1. INTRODUCTION
Over the past decades, in the research on information technology, Cloud computing [1] has become a prominent and fast-growing technology with the advantage of on-demand service and abundant resource availability. Although increased adoption of cloud computing services, privacy, and security becomes a significant constraint in the cloud environment [2]. In essence, the cloud environment requires several countermeasures activities, such as ensuring data privacy, data protection, data availability, location privacy of data, and secure transmission [3]. Despite the fact, both the external and internal threats are increasingly affecting the cloud environment. Hence, the intrusion detection system has been increasingly utilized by the cloud environment to secure the processing and stored data [4].

Recently, network security [5] and cloud security researches [6] have shown their increased interest in adopting machine learning techniques. In the machine learning-based security system, the abnormal and healthy behaviours are categorized based on the labelled traces from the training models. By extracting the different set of features, the machine learning and deep learning-based intrusion detection models [7, 8] ensure the security of the cloud environment. The machine learning and deep learning-based security model significantly detect the vulnerabilities with the reduced complexity and the reasonable cost. In recent years, there are numerous researches on the development of machine learning-based intrusion detection models. Although the machine learning techniques confront the different attack types over the abundant cloud environment, it fails to unknown attacks [9]. Hence, several existing researchers have presented the supervised and unsupervised learning-based security solutions [10, 11] to protect the data against the vulnerabilities. The data stored and executed in the cloud environment is significant to the cloud users with noxious intention; hence, providing security is prominent in the cloud environment with the support of machine learning algorithms [12]. Understanding the security measures that need to be taken by the cloud service provider is crucial while developing the cloud security model.

2. AN OVERVIEW OF CLOUD SECURITY THREATS
An emerging cloud computing technology not only offers different cloud services to the end-users but also leverages the increasing possibility of security risks and issues in the cloud environment [13]. By performing the illegal activities, the malicious individuals misuse the computing capability offered by the cloud. In essence, malicious individuals rent the virtual machines and launch the vulnerabilities on the virtual machines of other users within the cloud.

2.1. Security Vulnerabilities in the Cloud
Nowadays, hackers take advantage of the cloud computing service to conduct illegal activities in a distributed cloud environment. With the increased computing capability of cloud services, the hackers launch the attacks in a short period. For instance, by misusing the power of cloud computing, the malicious individuals begin Denial of Service (DoS) and brute force attacks in the cloud environment. In the cloud environment, security threats occur from within the organization as well as outside of the organization [14, 15]. Possible vulnerabilities can be created by a malicious insider in the cloud environment. This is mainly due to the unclear responsibilities and roles, lack of applying the need-to-know principles, weak enforcement of the role definition, Operating System (OS) or system vulnerabilities, application vulnerabilities, inadequate security of data, and Authentication, Authorization, and Accounting (AAA) vulnerabilities, [16]. Moreover, data breaches occur due to online cyber theft in the cloud environment. In the cloud environment, most of the stored data stealing is performed on

social networking sites such as Facebook, Twitter, MySpace. The online cyber thieves misuse the stolen passwords in terms of accessing the social account of the users as well as launching the malicious attacks to the users.

In the cloud environment, there are several security threats and issues that require significant attention among security researchers. Several security threats [17] involve the cloud account traffic hijacking, Internet Protocol (IP), data breaches, shared technology vulnerabilities, malicious insider, injection vulnerabilities, DoS, and so on. To the advantage of the ease of accessing the cloud service, there is a higher risk of hijacking or compromising the cloud user accounts. In the context of the IP, the inherent vulnerabilities involve the IP spoofing, DNS spoofing, and ARP spoofing. Data breaches occur while protecting the data between the cloud user and cloud service provider, including the intentional, malicious, and accidental data breaches in the cloud environment. In a cloud environment, hypervisor refers to the shared technology that is impacted by the inside and outside malicious individuals. In the cloud management layer, the injection vulnerabilities of LDAP injection, OS injection, and SQL injection flaw creates a negative impact on the multiple cloud users. Due to the multi-tenant nature of the cloud, any DoS attack affects all the tenants in the distributed cloud environment.

2.2. Attacks Scenarios in the Cloud

Nowadays, many organizations heavily rely on cloud computing to process, store, and share confidential information. To illegally access cloud resources, many hackers attempt to violate the security models, which prevents the cloud users from accessing the data in the cloud. The different kinds of attacks exist in the cloud [18, 19], including the Distributed Denial of Service (DDoS) Attack [20], malware injection attack, side-channel attack, Man-in-the-Middle (MITM) attack, wrapping attack, flooding attack, and so on.

3. CONVENTIONAL RESEARCHES ON CLOUD THREAT DETECTION AND CLASSIFICATION APPROACHES

In the cloud, previous researches have focused on applying different categories of the methods to handle security threats such as anomalies. Over the past decades, the statistics-based [21], knowledge-based [22], machine learning-based [23], and deep learning-based methods [24] have been widely utilized by the intrusion detection researchers. The statistical methods involve the seasonal decomposition method for filtering purposes, which significantly filter the trends present in the data. Then, by using the statistical metrics such as median and median absolute deviation, the researchers detect anomalous behaviour even when there are seasonal spikes in the data [25].

3.1. Machine Learning Technique Based on Anomaly Detection Approaches

In recent years, with the exponential amount of attacks generated in the cloud environment, there is a significant demand for developing potential solutions for cloud security. The cloud computing technology dramatically changes the data processing and data management across various computing fields. By integrating the machine learning algorithms with cloud computing technology, the existing researchers have improved the intrusion detection analysis [26, 27]. This section provides a brief review of supervised learning and unsupervised learning-based cloud security approaches.

3.1.1. Anomaly Detection System Using Supervised Learning Methods

To classify the unseen data, the supervised machine learning-based anomaly detection method exploits labeled instances which incorporate both the anomalous and normal sample for building the predictive model [28]. Machine learning techniques have the capability of discriminating abnormal and normal data with greater accuracy. The conventional rule-based cloud security solutions and firewalls become inadequate while handling the data in a multi-cloud environment. In recent years, the advancement of machine learning methods has received more attention from the researchers in developing the anomaly detection system. By employing the random forest and a linear regression algorithm, the work [29] categorize the attack by discovering the traffic of the abnormal. However, it lacks to determine the potential features for fine-grained analysis. To reduce a higher rate of false-negative, the work [30] introduces an imbalanced support vector machine-based anomaly detection model. It resolves the imbalanced dataset-related issues by performing dynamic weight allocation for a positive support-vector. It also helps to avoid the misclassification issue. However, it lacks to consider different types of attacks for classification. To address the problems of anomaly detection in the cloud environment, the work [31] initially segregates the cloud data into two types, such as anomaly and normal. Such data is fed into the multiple classifiers for acquiring individual decisions. Then, by aggregating the results of unique choices, it identifies the abnormal behaviour in the cloud infrastructure. However, it did not consider the VM performance profile for anomaly detection. By using a one-class support vector machine algorithm, the work [32] discovers the anomalies in the hypervisor. It can detect and respond to the unknown attacks online with the minimal cost of computing. To determine the anomalous VM in a cloud environment, the work [33] applies the Independent Components Analysis (ICA) on metric data, which helps to capture the independent components. It discovers the current state of the VM in a distributed system using a multi-class Bayesian classification model. However, it lacks to consider the location-related factor for decision-making. Distributed Denial of Service (DDoS) attack is the most severe attack that significantly affects the performance of the cloud environment. C.4.5-based DDoS threat detection model associated with signature detection methods for identifying the signatures of the DDoS attack. The combination of decision trees and signature detection techniques offer greater detection accuracy. However, it lacks to select a vital feature for threat detection [7]. The hybrid DDoS attack detection framework uses an incremental learning method for discovering attacks. Initially, it collects the data from the client-side and applies the forward feature selection algorithm for extracting the essential features. According to the divergence test, it identifies the attack. On the proxy side, it employs random forest, naïve Bayes, k-nearest neighbors (K-NN), multilayer perceptron (MLP), and decision tree for achieving more significant results [34]. To enhance the business of financial service providers, the work [35] applies the Decision Tree-based Risk Prediction (DTRP) algorithm for detecting the security risk in the cloud environment. However, it induces a workload while handling large-scale data.

3.1.2. Anomaly Detection System Using Unsupervised Learning Methods

This method does not require any training data. It assumes two things about the data, i.e., Only a small percentage of data is abnormal, and any anomaly is statistically different from the normal samples. Based on the above assumptions, the data are then clustered using the similarity measure and the data points, which are far from clusters considered as anomalies. In essence, the clustering methods do not rely on the labelled data for detecting the various anomalous behaviour. The clustering-based anomaly detection becomes an active research area owing to its independent nature and adaptation to different categories of anomalies [36]. The work employs a density-based clustering method to discover application anomalies. Additionally, it leverages application-related knowledge in determining the most useful features to build the anomaly detection model. However, it fails to use the knowledge of multiple applications for generalization [37]. To mitigate the attack in the cloud, a clustering-based anomaly detection framework for discovering the unknown changes of behavior. However, it needs to focus on the reduction of the false-positive rate for acquiring promising results in the clustering method [38]. By employing the enhanced sequential K-means clustering algorithm, the work [39] detects the anomalies in the cloud environment by reducing the false alarm rate. It focuses on the interaction between the VM and resource usage to ensure the secured cloud environment. However, it requires a parameter tuning mechanism for acquiring reasonable results. The work involves three main phase identification of trend patterns, feature transformation, and behavior modeling to attain better accuracy in abnormal behavior detection. Initially, it applies the Mann-Kendall test for identifying the significant trends. Further, it employs the entropy measures for selecting the relevant set of the feature over the large-scale data. Finally, it uses a DBSCAN method for identifying abnormal behavior. However. It lacks to consider the correlation between abnormal behavior while detecting an anomaly in a distributed environment for promising solutions [40]. By employing the clustering method, the work [41] processes the stream data that arrives from the VM in the cloud environment. It splits the incoming stream data into sub-stream then apply the clustering method for improving the scalability. It has taken into account the relentless changes in the system for identifying unknown anomalies. However, it fails to consider the other parameter for avoiding false alarm rates. By utilizing the supervised and unsupervised learning techniques, the work [42] attempts to enhance the threat detection performance and classification accuracy. It ensures the customized security for each user in the cloud environment by handling the massive amount of data with the presence of an unknown and new threat. Yet, it struggles to collect the labeled data from the network environment owing to the time constraints and privacy issues.

3.2. Existing Research Works on Deep Learning Based Anomaly Detection

Deep learning is a kind of machine learning method that incorporates multiple hidden layers and nodes for representing the learning process. It is capable of processing large-scale data and has identified as the most promising solution for anomaly detection. This section provides a review of deep learning-based anomaly detection methods. To resolve the challenges of anomaly detection, the work [43] integrates the variational auto-encoders with the Gated Recurrent Unit (GRU) for identifying the underlying pattern of the time series data. It reduces the false positive rate by using a tolerance module. However, it lacks to use cross-event knowledge for analyzing the structure of anomalies. The hybrid network anomaly detection model combines the Convolutional Neural Network (CNN) and Grey Wolf Optimization (GWO) for improving the detection accuracy. By leveraging Improved-GWO, it selects the most critical features for maintaining the optimal set of features, which helps to reduce the error rate. By using the improved-CNN, it classifies the anomalies in the network [44]. Ensemble learning-based anomaly detection model employs Unscented Kalman Filter and Restricted Boltzmann Machine for selecting potential features over the large-scale cloud data. To accurately detect anomalies, it applies the Artificial Bee Colony-based Fuzzy C-means clustering method, which ensures the optimal results. The resulting clusters are used to discriminate the normal events from abnormal [45]. To identify the new and unknown attacks, the work [46] integrate Deep Belief Network (DBN) and Restricted Boltzmann Machine (RBM) for reducing the false-negative rate. By using RBM, it performs the feature reduction in an unsupervised manner. By using the DBN method, it detects the anomalies in the environment. Yet an anomaly detection based on deep learning requires further enhancement in the feature reduction process for improving the speed of detection. Deep learning-based DDoS attack detection framework [47] use a pattern matching mechanism for discovering the anomalous behavior. Notably, it uses Cellular Neural Network(CNN) for classifying the anomalies in the cloud environment with a higher rate of DDoS attack detection. However, it lacks to identify the relevant features in the environment. Multi-Layer Perceptron (MLP)-based DDoS attack detection model in [48] integrates the MLP model and feature selection method for reducing the detection errors. It presents a feedback mechanism for recognizing the detection errors on detection results. It focuses on the changeable traffic problem in the system and fails to handle the false-negative issues.

3.2.1. Review on Transfer Learning Based Anomaly Detection Approaches

To detect the anomalous behavior, most of the research works apply traditional machine learning methods which require a large-scale labeled instance for learning the anomalous behavior. However, in real-time, the unpredictability and rapid pace of cyberattacks make it unrealistic because the collection of an adequate number of labeled instances of continuously evolving attacks is impossible. It demands a need for transfer learning method for anomalous behavior detection. The CNN-based transfer learning model [49] detect the anomalies in a time series environment. It exploits the

Table 1: Comparison of Different Machine Learning based Cloud Security Researches

Cloud Security Model	Targeted Attacks	Techniques	Merits	Limitations
Security incident detection	Anomalies	Complex event processing rule and machine learning	Resolves the security issues in multi-tenant cloud	Detects anomalies with increased false positives
LOF-based Adaptive Anomaly Detection Scheme	Anomalies	Local Outlier Factor (LOF) algorithm	Alleviates the effort of training data collection and improves contextual detection of anomalies	Leads to inaccurate detection of gradual change anomalies as normal behaviors
Frequent Pattern-based Anomaly Detection	Anomalies	Frequent pattern mining and re-sampling	Detects malicious activities by reducing the false positive rate	Lacks to support attack detection when there is a change in the user's normal behaviors
Fuzzy logic based defense mechanism	DDoS attacks	Fuzzy Logic	Detects malicious packets based on the predefined rules	Fails to detect new attack types in the cloud
Ensemble-based multi-filter feature selection	DDoS attacks	Ensemble Model, Decision Tree, Information gain, Gain ratio, Chi-squared, and Relief-F	Improves attack detection accuracy by utilizing multiple filters for optimal feature selection	Fails to support the diversified attack detection
Cloud-based cyber risk management	Cyber risks	Decision Tree-based Risk Prediction (DTRP) algorithm	Accomplishes high quality of cyber risk management in the financial industry	Increases computational complexity
SYN Flood Attack Detection	SYN Flood Attack	Support Vector Machine	Detects the DoS attacks through effective feature extraction	Lacks to detect the different type of attacks
SVM-based DoS attack Detection	DoS attacks	Support Vector Machine	Detects the attacks in the dynamic environment and also, identifies the compromised virtual machines	Removal of relevant data as noisy data misguides the classification model
Trusted Ransomware detection	Ransomware	Random Forest	Based on the analysis of volatile memory, detects ransomware	Distinct feature extraction leads to inaccurate ransomware detection
Trust-Based Access Control	Cloud security risks	Logistic regression, K-nearest neighbor, Naive Bayes, and decision tree	Ensures secure cloud access	Regardless of the role of the cloud components leads to inaccurate risk management

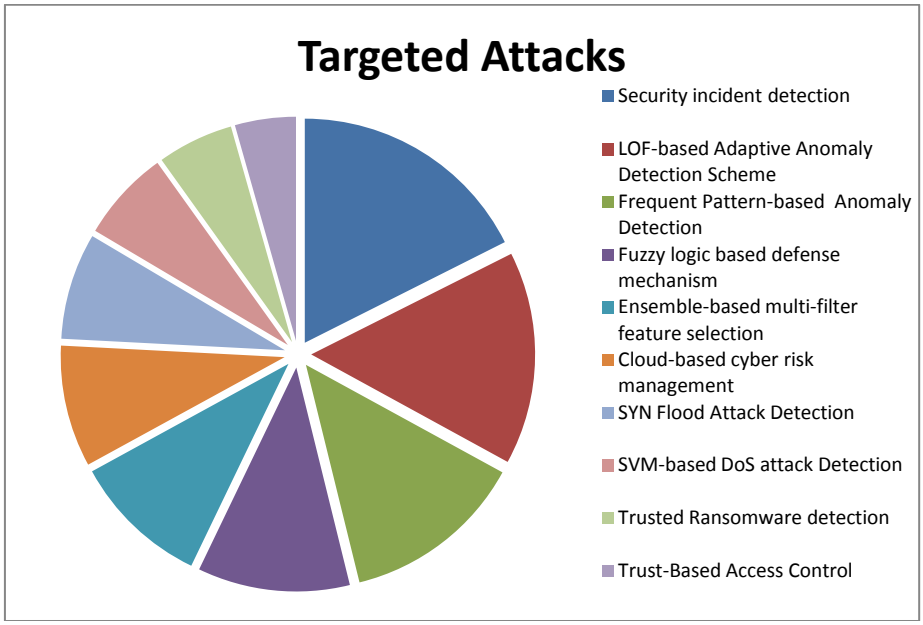

Fig 1:Cloud Security Models-Targeted Attacks

weights of the base model that pre-trained on a massive amount of data. Then, it fine-tunes the weights of the model on multivariate and univariate data for discovering the unknown anomalies in the time series environment. By

employing the transfer learning method, the work [50] detects the time series anomalies, where the labeled examples of source domain are transferred to the target domain for determining infrequent and unknown anomalies. It applies the dynamic time warping method for evaluating similarity scores between target and source domains to build an anomaly classification model. To identify the unknown attack and their behavior on the network, the work [51] employs a Feature-based transfer learning approach. It detects the variants of attacks in the system based on HeTL. To identify the new attacks accurately, the work [52] evaluates the relationship between the already recognized attack and new attack using the cluster-based transfer learning method. It enhances the performance of detecting unseen and fresh attacks on the network environment. Active Transfer Anomaly Detection (ATAD) approach combines active learning and transfer learning methods for discovering time series anomalies. By applying the active learning method, it computes the informational label for a small set of instances in unlabeled data [53]. The hybrid attack detection model classifies the different types of intrusions in the cloud environment using the transfer learning method. Initially, it trains the learning model on a non-cloud dataset and applies the pre-trained model on the cloud dataset for detecting the intrusions in a cloud environment [54]. Table 1 reviews several machine learning algorithms based on cloud security approaches.

4. CHALLENGES AND FUTURE DIRECTIONS FOR THE MACHINE LEARNING BASED CLOUD SECURITY

Over the decades, cloud computing has attracted by the intruders along with the Information Technology (IT) organizations. Due to the complex architecture of the cloud, developing a cloud-based security model requires additional requirements to improve the performance of the application running in the cloud server compared to the traditional server. The current researchers have presented different security solutions using machine learning and deep learning algorithms to protect the cloud environment from a variety of attacks. The cloud security model confronts several challenges while applying machine learning and deep learning techniques [6]. This section discusses the research challenges faced by security researchers and several future research directions for enhancing cloud security.

5. CONCLUSION

With the advantage of quick deployment, easy access, massive storage space, and cost-efficiency, the adoption of cloud computing technology is continuously growing. The increased security concerns become the primary obstacle to the adoption of the cloud computing paradigm. Hence, security creates significant attention among cloud security practitioners and researchers. Still, there is a considerable gap in providing adequate security against the threats, vulnerabilities, and attacks in the cloud. This work surveyed the cloud security attacks and existing different countermeasures for the virtualized cloud environment. Moreover, this work has presented numerous machine learning and deep learning-based security models to address the security challenges in the cloud. Finally, the discussion of the research challenges and future directions in the cloud security motivate the researchers to focus on developing security from that perspective.

6. REFERENCES

[1] Varghese, B. and Buyya, R., "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Vol.79, pp.849-861, 2018

[2] Almorsy, M., Grundy, J. and Müller, I., "An analysis of the cloud computing security problem", arXiv preprint arXiv:1609.01107, 2016

[3] Singh, S., Jeong, Y.S. and Park, J.H., "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications, Vol.75, pp.200-222, 2016

[4] Mishra, P., Pilli, E.S., Varadharajan, V. and Tupakula, U., "Intrusion detection techniques in cloud environment: A survey", Journal of Network and Computer Applications, Vol.77, pp.18-47, 2017

[5] Liu, H. and Lang, B., "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey", Applied Sciences, Vol.9, No.20, p.4396, 2019

[6] Kumar, R.S.S., Wicker, A. and Swann, M., "Practical machine learning for cloud intrusion detection: challenges and the way forward", In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, pp.81-90, 2017

[7] Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y., "DDoS attack detection using machine learning techniques in cloud computing environments", IEEE 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), pp.1-7, 2017

[8] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C., "Machine learning and deep learning methods for cybersecurity", IEEE Access, Vol.6, pp.35365-35381, 2018

[9] Khorshed, M.T., Ali, A.S. and Wasimi, S.A., "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation computer systems, Vol.28, No.6, pp.833-851, 2012

[10] Wani, A.R., Rana, Q.P., Saxena, U. and Pandey, N., "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques", IEEE Amity International Conference on Artificial Intelligence (AICAI), pp.870-875, 2019

[11] Pitropakis, N., Panaousis, E., Giannetsos, T., Anastasiadis, E. and Loukas, G., "A taxonomy and survey of attacks against machine learning", Computer Science Review, Vol.34, p.100199, 2019

[12] Papernot, N., McDaniel, P., Sinha, A. and Wellman, M., "Towards the science of security and privacy in machine learning", arXiv preprint arXiv:1611.03814, 2016

[13] Khan, M.A., "A survey of security issues for cloud computing", Journal of network and computer applications, Vol.71, pp.11-29, 2016

[14] Dahbur, K., Mohammad, B. and Tarakji, A.B., "A survey of risks, threats and vulnerabilities in cloud computing", In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications, pp.1-6, 2011

[15] Singh, A. and Chatterjee, K., "Cloud security issues and challenges: A survey", Journal of Network and Computer Applications, Vol.79, pp.88-115, 2017

[16] Zeadally, S., Yu, B., Jeong, D.H. and Liang, L., "Detecting insider threats: Solutions and trends" Information security journal: A global perspective, Vol.21, No.4, pp.183-192, 2012

[17] Hong, J.B., Nhlabatsi, A., Kim, D.S., Hussein, A., Fetais, N. and Khan, K.M., "Systematic identification of threats in the cloud: A survey", Computer Networks, Vol.150, pp.46-69, 2019

[18] Kumar, R. and Goyal, R., "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey", Computer Science Review, Vol.33, pp.1-48, 2019

[19] Juliadotter, N.V. and Choo, K.K.R., "Cloud attack and risk assessment taxonomy", IEEE Cloud Computing, Vol.2, No.1, pp.14-20, 2015

[20] Alarqan, M.A., Zaaba, Z.F. and Almomani, A., "Detection Mechanisms of DDoS Attack in Cloud Computing Environment: A Survey", In International Conference on Advances in Cyber Security, Springer, pp.138-152, 2019

[21] Lin, W.C., Ke, S.W. and Tsai, C.F., "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors", Knowledge-based systems, Vol.78, pp.13-21, 2015

[22] Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S. and Herrera, F., "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems", Expert Systems with Applications, Vol.42, No.1, pp.193-202, 2015

[23] Buczak, A.L. and Guven, E., "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Communications surveys & tutorials, Vol.18, No.2, pp.1153-1176, 2016

[24] Kwon, D., Kim, H., Kim, J., Suh, S.C., Kim, I. and Kim, K.J., "A survey of deep learning-based network anomaly detection", Cluster Computing, pp.1-13, 2017

[25] Hochenbaum, J., Vallis, O.S. and Kejariwal, A., "Automatic anomaly detection in the cloud via statistical learning", arXiv preprint arXiv:1704.07706, 2017

[26] Gulenko, A., Wallschläger, M., Schmidt, F., Kao, O. and Liu, F., "Evaluating machine learning algorithms for anomaly detection in clouds", IEEE International Conference on Big Data (Big Data), pp.2716-2721, 2016

[27] Habeeb, R.A.A., Nasaruddin, F., Gani, A., Hashem, I.A.T., Ahmed, E. and Imran, M., "Real-time big data processing for anomaly detection: A Survey. International Journal of Information Management, Vol.45, pp.289-307, 2019

[28] Jia, W., Shukla, R.M. and Sengupta, S., "Anomaly Detection using Supervised Learning and Multiple Statistical Methods", 18th IEEE International Conference On Machine Learning And Applications (ICMLA), pp.1291-1297, 2019

[29] Salman, T., Bhamare, D., Erbad, A., Jain, R. and Samaka, M., "Machine learning for anomaly detection and categorization in multi-cloud environments", IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp.97-103, 2017

[30] Wang, G., Yang, J. and Li, R., "Imbalanced SVM-Based Anomaly Detection Algorithm for Imbalanced Training Datasets", Etri Journal, Vol.39, No.5, pp.621-631, 2017

[31] Alguliyev, R.M., Aliguliyev, R.M. and Abdullayeva, F.J., "Hybridisation of classifiers for anomaly detection in big data", International Journal of Big Data Intelligence, Vol.6, No.1, pp.11-19, 2019

[32] Watson, M.R., Marnerides, A.K., Mauthe, A. and Hutchison, D., "Malware detection in cloud computing infrastructures", IEEE Transactions on Dependable and Secure Computing, Vol.13, No.2, pp.192-205, 2015

[33] Wang, G., Yang, J. and Li, R., "An anomaly detection framework based on ICA and Bayesian classification for IaaS platforms", KSII Transactions on Internet and Information Systems (TIIS), Vol.10, No.8, pp.3865-3883, 2016

[34] Hosseini, S. and Azizi, M., "The hybrid technique for DDoS detection with supervised learning algorithms", Computer Networks, Vol.158, pp.35-45, 2019

[35] Gai, K., Qiu, M. and Elnagdy, S.A., "Security-aware information classifications using supervised learning for cloud-based cyber risk management in financial big data", IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp.197-202, 2016

[36] Ariyaluran Habeeb, R.A., Nasaruddin, F., Gani, A., Amanullah, M.A., Abaker Targio Hashem, I., Ahmed, E. and Imran, M., "Clustering-based real-time anomaly detection—A breakthrough in big data technologies", Transactions on Emerging Telecommunications Technologies, p.e3647, 2019

[37] Elsner, D., Aleatrati Khosroshahi, P., MacCormack, A.D. and Lagerström, R., "Multivariate Unsupervised Machine Learning for Anomaly Detection in Enterprise Applications", In Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019

[38] Gander, M., Felderer, M., Katt, B., Tolbaru, A., Breu, R. and Moschitti, A., "Anomaly detection in the cloud: Detecting security incidents via machine learning", InInternational Workshop on Eternal Systems, Springer, pp.103-116, 2012

[39] Abdelsalam, M., Krishnan, R. and Sandhu, R., "Clustering-based IaaS cloud monitoring", IEEE 10th International Conference on Cloud Computing (CLOUD), pp.672-679, 2017

[40] Zhang, X., Meng, F. and Xu, J., "Perfinsight: A robust clustering-based abnormal behavior detection system for large-scale cloud", IEEE 11th International Conference on Cloud Computing (CLOUD), pp.896-899, 2018

[41] Sauvanaud, C., Silvestre, G., Kaâniche, M. and Kanoun, K., "Data stream clustering for online anomaly detection in cloud applications", IEEE 11th European Dependable Computing Conference (EDCC), pp.120-131, 2015

[42] Kim, H., Kim, J., Kim, Y., Kim, I. and Kim, K.J., "Design of network threat detection and classification

based on machine learning on cloud computing", Cluster Computing, Vol.22, No.1, pp.2341-2350, 2019

[43] Nedelkoski, S., Cardoso, J. and Kao, O., "Anomaly Detection and Classification using Distributed Tracing and Deep Learning", 2018

[44] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A.Y. and Ranjan, R., "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks", IEEE Transactions on Network and Service Management, Vol.16, No.3, pp.924-935, 2019

[45] Garg, S., Kaur, K., Batra, S., Aujla, G.S., Morgan, G., Kumar, N., Zomaya, A.Y. and Ranjan, R., "En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment", Journal of Parallel and Distributed Computing, Vol.135, pp.219-233, 2020

[46] Alrawashdeh, K. and Purdy, C., "Toward an online anomaly intrusion detection system based on deep learning", 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp.195-200, 2016

[47] Yang, Z.X., Qin, X.L., Li, W.R. and Yang, Y.J., "A DDoS detection approach based on CNN in cloud computing", In Applied Mechanics and Materials, Vol.513, pp.579-584, 2014

[48] Wang, M., Lu, Y. and Qin, J., "A dynamic MLP-based DDoS attack detection method using feature selection and feedback", Computers & Security, Vol.88, p.101645, 2020

[49] Wen, T. and Keyes, R., "Time Series Anomaly Detection Using Convolutional Neural Networks and Transfer Learning", arXiv preprint arXiv:1905.13628, 2019

[50] Vercruyssen, V., Meert, W. and Davis, J., "Transfer learning for time series anomaly detection", In CEUR Workshop Proceedings, Vol.1924, pp.27-37, 2017

[51] Zhao, J., Shetty, S. and Pan, J.W., "Feature-based transfer learning for network security", In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp.17-22, 2017

[52] Zhao, J., Shetty, S., Pan, J.W., Kamhoua, C. and Kwiat, K., "Transfer learning for detecting unknown network attacks", EURASIP Journal on Information Security, Vol.2019, No.1, p.1, 2019

[53] Zhang, X., Kim, J., Lin, Q., Lim, K., Kanaujia, S.O., Xu, Y., Jamieson, K., Albarghouthi, A., Qin, S., Freedman, M.J. and Xiong, Y., "Cross-dataset time series anomaly detection for cloud systems", In 2019 {USENIX} Annual Technical Conference ({USENIX}{ATC} 19), pp.1063-1076, 2019.

[54] Samreen, F., Blair, G.S. and Elkhatib, Y., "Transferable Knowledge for Low-cost Decision Making in Cloud Environments", arXiv preprint arXiv:1905.02448, 2019