SEYBOLD Report
ISSN: 1533 - 9211
https://seyboldreport.net/

A REVIEW OF COMPARATIVE ANALYSIS OF CLOUD-BASED ATTACK AND ITS DETECTION USING DIFFERENT MACHINE LEARNING ALGORITHMS

Sudha D
Research Scholar, Jain University (Deemed to be University) ,
School of Compuer science and Information Technology Department of MCA
sudhashinu@gamil.com

Dr.Bhuvana J
Associate Professor, Jain University (Deemed to be University),
School of Computer science and Information Technology Department of MCA
j.bhuvana@jainuniversity.ac.in

Abstract --- "Cloud computing" (CC) means providing on-demand network resources, especially data storage and processing capabilities, without special user management or direct management. CC is a set of modern public and private data centers that provide clients with an integrated platform over the Internet. Machine learning (ML) is the study of computer algorithms that improve themselves in practice. In this research review, we analyze CC security threats, problems, and solutions using one or more ML algorithms. We review a variety of machine learning (ML) techniques such as mapping, viewing, compliance and enhanced learning to respond to cloud security challenges. The performance of each technology is then compared based on its attributes, advantages and disadvantages.

Index Terms—

I. INTRODUCTION

Cloud computing, a virtualization technology, allows us to design, configure and modify applications online. Hard drives, software programs, databases, and development platforms are all components of cloud technology. A network or the Internet is called a "cloud". This is a system that replaces remote Internet servers instead of local hard drives while storing, managing and retrieving data. Thus, everything you have selected, including files, photos, text, audio, video, etc., can be considered data.

There are four main types of clouds:

The public cloud is operated by third parties, provides cloud services to the public via the Internet, and is overpaid through a fee-paying option. They provide ways to reduce IT infrastructure costs and are becoming practical options for managing peak demand in local infrastructure. When small start their operations, they rely solely on a public infrastructure to meet their IT requirements without investing a lot of initial money, and choose the public cloud as their preferred option. Multi-user sharing is one of the key features of the public cloud. Public clouds are designed to serve not only one specific client but also many users. Users need a

virtual computing environment that is isolated from other users and possibly isolated.

Private cloud is a distributed system operated on a private infrastructure that gives users access to dynamically allocated computer resources. In the private cloud, you may have additional plans to control cloud usage, which overload the various departments or areas of your organization in proportion, instead of the pay-eye-your-yourself method used in the private Cloud.

When you combine public and private cloud resources, you develop a distributed system called a hybrid cloud. For this reason, these are also known as binary clouds. The great disadvantage of expanding private deployment is that it cannot effectively handle business peak loads as required. In this case, you need a public cloud. As a result, hybrid clouds take advantage of both public and private clouds.

II. Cloud Computing Services

There are three different types of cloud computing services:
SaaS (Software as a Service):
SaaS is a way to deliver services and applications over the Internet. We access the software via the Internet and are free from complex software and hardware management. Instead of installing andining, we do not need to install or maintain the software on our own computers or data centers. As a result, you can save on both hardware and software management.

PaaS (Platform as a Service):
PaaS is a subcategory of cloud computing that provides platforms and environments for developers to create online apps and services. PaaS services are stored in the cloud, making it easy for users to access them through a web browser. PaaS providers host hardware and software on their own infrastructure. As a result, PaaS prevents users from having to install their own hardware and software to create or run new applications. As a result, the hardware does not affect the creation or distribution of the program.

IaaS (Infrastructure as a Service):
IaaS is a service delivery paradigm that outsources the provision of computer infrastructure to support a variety of processes. IaaS is a service that typically provides infrastructure such as networking hardware, devices, databases, and web servers from outside to business. This is also called "Service as Hardware" (HaaS).

III. IMPLEMENTATION OF CLOUD

Cloud is one of the most commonly used technologies due to its efficient infrastructure and deployment architecture. Cloud users can access the computer resource pool over the Internet. Scalability, flexibility, efficient communication, time and cost savings are key advantages of cloud implementation. Enabling secure data storage and access within the cloud is providing

security.

Safe, effective and flexible data sharing with users with different privileges is key to cloud computing. The new public key password system is used to generate code text of the same size at all times to effectively aggregate secret keys with duplication permissions. Anyone with access to a secret key can disclose a set of aggregate keys of a certain size, and can flexibly choose the set of code text while retaining the privacy of other encrypted files.[12][7]

Cloud computing seems really simple to the consumers of cloud as in access cloud, place or retrieves required data that's all. But the internal cloud is built on three very important layers.[11] Those layers are named as software as a service (SaaS), Platform as a service (Paas) and Infrastructure as a service (IaaS). Various cloud service providers provide different kind of services based on those layers. On the first level that is software as services, various applications reside that provides an interface to end users. This layer generally allows access to internal data with some authentication mechanism. The second layer is a platform as a service, this layer contains various mappings of users request to the required resource that resides on cloud computing. The final layer is infrastructure, which most of the time includes virtual machines and other infrastructure that users can utilise to request calculations. Each cloud layer has its own vulnerabilities. Similar to software as a service, layer relies on authentication to verify the identity of the document's owner, but this can be compromised if another person has access to the security code that is being used for authentication.

III Cloud-Based Attack [attacks and solution]

Distributed Denial of Service (DDoS): As more companies rely on cloud-based services, DDoS (Distributed Denial of Service) attacks (also known as DDoS attacks) are becoming a common and crucial attack on the cloud, which proves to be quite devastating. An assault known as a distributed denial of service (DDoS) consumes all available cloud resources, rendering them useless to other customers.

A whole internet user base is affected by a successful distributed denial of service assault, which is a very noteworthy occurrence. As a result, it is a popular tool for hacktivists, cyberterrorists, extortionists, and anybody else trying to further an agenda or make a point. DDoS assaults can result in lost sales, destroy customer confidence, force companies to shell out enormous sums in reparations, and permanently harm a company image.

Malware Injection Attack: A cyber attack using malicious code and services on a cloud computing-based system is referred to as a "malware injection attack" or "malware in the cloud." The numerous cloud-based systems are becoming prime targets for cyberattacks thanks to cloud malware. The following are the most typical cloud-based systems that are vulnerable to cloud-based systems:

• Open cloud-based systems on the internet; • Standard and simple to learn cloud-based systems; • Cloud-based systems are made up of several components such virtual machines

(VMs), storage buckets, and containers.
A cloud malware injection attack is used to target the cloud computing platforms. Here, a hacker will attempt to introduce a harmful service or virtual machine inside the cloud-based system. As a result, it generates malicious service implementation modules or virtual machine instances associated to either SaaS.

Phishing attack
Phishing is a form of social engineering assault that is frequently used to obtain user data, such as login credentials and credit card details. It takes place when an attacker convinces a victim to open an email, instant message, or text message by disguising themselves as a reliable source. The recipient is subsequently duped into clicking a malicious link, which can result in the installation of malware, the freezing of the machine as part of a ransomware assault, or the disclosure of sensitive information.
There are various phishing scams.
1. Email phishing scams
2. Spear phishing
Email phishing is a game of numbers. An attacker who sends thousands of false communications can amass significant information and substantial sums of money, even if only a small percentage of recipients fall for the fraud.

SQL Injection Attack: Structured Query Language (SQL) is a language used to manage and manipulate data in databases. Since its introduction, SQL has gradually made its way into numerous private and public databases. In order to fool the systems into performing unexpected and undesirable actions, SQL injection (SQLi), a sort of cybersecurity attack, attacks these databases. There are several techniques to conduct SQL injection attacks:
1)Unsanitized Input
2)Blind SQL Injection
3)Out-of-Band Injection

Man in the Middle Attack: A type of cyber eavesdropping, Man in the Middle Attack. Hackers try to eavesdrop on communications between the source and the destination. A "third individual listening to a conversation between two persons in the middle of a communication channel" is what is meant by the phrase "Man in the Middle Attack." A successful MitM attack requires the hacker to remain undetectable to the target. The goal of the interception is to either steal, listen in on, or alter the data for bad intentions, like extortion. several attack types:
Interception - The interruption of data before it reaches the destination
Decryption - The interruption of data at the destination without the notice of the receiver

V. Machine Learning Algorithms and cloud Security
The logical examination of computations and quantitative models used by computer systems to complete a task without the need for explicit guidance, relying upon models, or

acceptance is known as machine learning (ML). The term "automated reasoning" refers to it [19]. Due to its significance to clouds, ML will soon be used by all clouds [21]. Instead of demonstrating how ML may improve distributed computing security, this section will look at asset designation and focus [20].

Due to the increase of critical information in the cloud together with the growth of general information in the cloud, more security in CC is required. The strategies outlined in this section employ more accurate risk detection to improve cloud security [22]. We begin by providing a comprehensive method for calculating risks and dangers by summing the seriousness of each hazard. Next, we go through threat management strategies that create a half-and-half threat detection model by combining signature identification with anomaly detection [23].

Types of ML Algorithms

Machine learning is an application of artificial intelligence (AI) that enables machines to automatically learn from experience and improve. We can classify machine learning as follows:

- Supervised
- Unsupervised
- Semi-supervised
- Reinforcement

Compared to cloud computing, machine learning is a relatively recent technology. Although the development of an organization depends on both technologies, their combined power is more substantial. Machine learning develops intelligent hardware or software, whereas cloud computing provides storage and security for access to these applications.

Supervised learning in machine learning aims to develop a function that translates a contribution to the yield subject to process data yield sets. It encourages the naming of the data that many preparation models use. Managed learning is an essential aspect of data science [21]. Starting a limit using prepared data is a need of the ML task known as administered learning, which calls for multiple getting ready models.

Supervised Neural Network: A supervised neural network has a known information return. The expected and actual yields of the neural system are compared. The parameters are changed in light of the fault before the neural system is addressed once more. The administered neural system is utilized by a feed-forward neural system [20].

K-Nearest Neighbor (K-NN) is an easy-to-use ML computation that may be applied to characterization and regression issues. The yield of a regression issue is a real number, or a decimal value. For instance, it uses the information in the table below to calculate an individual's weight based on height.

Support Vector Machine (SVM) is a controlled ML method that is applied to both data

collection and relapse problems. It is typically applied to characterisation problems. A frontier dividing the two classes is the SVM classifier (hyper-plane).

Naive Bayes: A controlled ML algorithm that acknowledges that highlights are factually free and utilises Bayes' theorem. Despite this presumption, it has proven to be a classifier that produces useful results.

Unsupervised learning is a sort of machine learning method used to infer conclusions from datasets made up of data without clearly defined responses. Cluster analysis, which is used for exploratory information analysis to find hidden examples or grouping in the information, is the unsupervised learning technique that has received the most recognition [58].

Unsupervised Neural Network: The neural network has no prior knowledge of the information yield. The system's main job is to categorise the information based on a number of commonalities. The neural system confirms the relationship between various information sources and gatherings.

One of the simplest and most well-known unsupervised ML techniques is K-Means. The K-means method detects k numbers of centroids, then quickly generates each data point to the closest cluster while keeping the centroids as minimal as is reasonable given the current situation.
Singular Value Decomposition (SVD): One of the most popular unsupervised learning algorithms, at the core of various proposals and dimensionality reduction frameworks that are crucial to multinational corporations like Google, Netflix, and others.

A machine learning approach called semi-supervised learning combines a lot of unlabeled input with little recognized data during training. Semi-supervised learning encompasses both supervised and unsupervised learning. Semi-supervised learning's aim is to set up operations that employ a combination of labeled and unlabeled input in order to examine how doing so could change the learning behavior.

Reinforcement learning (RL), a subfield of machine learning (ML), emphasizes the use of situations and actions by programmers to better understand the overall return. Unsupervised learning and supervised learning, of which RL is one, are the other two principal ML ideal models. One of the challenges that develops in RL and not only in classrooms is the exchange of the test and abuse.

Literature Review

[1] The study addressed email-text-based phishing attacks using SVM, NB, and LSTM methods. The authors also explained that in COVID-19 situations, all tasks are handled at home, and 99% of the data is sent and received by email. Attackers are active and use phishing

techniques such as text messages, messengers, phones, emails, and even search engine results manipulation. The authors' proposed solution is to quickly identify phishing or non-phishing data using desired properties based on maps and deep learning algorithms, and to eliminate errors through subsequent text processing. We used SVM, NB, and D Learning LSTM algorithms to detect and eliminate phishing attacks with 99%, 97%, and 98% accuracy.

[2] Proposes a technology to detect DDoS (Distributed Denial of Service) attacks that disrupt network connections using the power of systems infected with multiple malware. Here are two approaches to detecting DDoS attacks. 1) Mathematical Simulation 2) Models for Machine Learning. Here, we build machine learning models to detect DDoS attacks using logistic regression and nail base models. The authors concluded that the performance of machine learning models was slightly better than that of mathematical models. 100% accuracy was achieved for machine learning models and 99.7% for mathematical models.

[3] We presented and modeled the Bayesian Belief Network (BBN) model to predict Man-in-the-Middle attacks. There are a total of 26 nodes, and each node within the network represents a different type of attack. The authors trained and tested the proposed BBM model through experiments, which showed a high residual log thickness value, a 26.21 residue log thinity percentage. In addition, we achieved a remaining log advantage rate of 99.16%. The authors have proposed an innovative BBN method with 99% accuracy to predict MHM attacks.

The study [4] aimed to demonstrate the effectiveness of anomaly detection in industrial control systems by creating a project setup with typical industrial components. They trained a behavioral model using data from normal system operations and then simulated Man-in-the-Middle attacks to test the anomaly detection approach. By comparing the attack-generated data with the established behavior model, the study successfully identified significant deviations indicative of an attack. While acknowledging the need for further exploration, the research highlighted the potential of anomaly detection for bolstering cybersecurity in industrial contexts, hinting at its application to various types of attacks beyond Man-in-the-Middle, such as Denial-of-Service and Replay Attacks..

This paper [5] uses SVM, the Decision Tree, and Logistic Regression to counter DDOS attacks. The training data set was provided by the Canadian Institute of Cyber Security. Using nine parameters and one attribute observed through the data, the model learns the situation before predicting the data. Logistic regression, critical tree, and SVM showed accuracy values of 0.97, 0.82, and 0.59, respectively.

[6] It uses a variety of machine learning techniques, such as SVM, nail base, and IRF, to perform classification operations. The data set was created using SNORT's intrusion detection system. The next step is attribute extraction and data correction. Cross-verification of the classifications used after training was carried out using 10-poles cross-validation for the

selected parameters. The performance is then compared with the algorithm-generated confusion matrix. According to research results, the accuracy of SVM, RF, and NB is 99.7%, 97.6%, 98%, respectively.

[7] The paper used the DT (Decision Tree) method of data collection, which automatically identifies the event and labels whether the event has been detected. We identified potential cyber-attacks from smart grid and sports-related data, and analyzed cases that were originally described for different reasons by infiltration. After that, we studied the attack scenario to learn more about how it could penetrate endpoint nodes. Finally, we learned data sets using DT algorithms and machine learning techniques. Using the algorithm, the prediction achieved 83% accuracy, and the map learning model surpassed itself.

8] This paper explores the use of various machine learning classifier features for the purpose of identifying malware. The authors integrated a variety of small data sets to create a unique data set. Python was used to implement the proposed system. The course starts with attribute creation and model selection, followed by using machine learning models to distinguish malicious SQL queries from legitimate payloads. The application reads the training data set from a CSV file, and the classifier uses the data as part of the learning process. The AdaBoost Classifiers, SGD, Random Forest, Decision Tree, Tensorflow, Linear Classificers, Tenserflow Boosted Trees, and Deep Neural Networks (DNNs) have achieved accuracy levels of 99.3%, 99.1%, 99,8%, 99,52%, 97.3%, 99,5%, and 97.6% with eight features, respectively.

VI. COMPARITIVE STUDY

Phishing Attack:

Dataset: Email-based

Machine Learning Algorithms: Support Vector Machine (SVM) achieved an accuracy of 99.62%, while Naive Bayes (NB) achieved an accuracy of 98%.

SVM appears to outperform NB in this case.

DDoS Attack (CAIDA Dataset):

Dataset: CAIDA Dataset

Machine Learning Algorithms: Both Logistic Regression and Naive Bayes achieved 100% accuracy.

Both algorithms performed exceptionally well on this dataset, achieving perfect accuracy.

MitMA Attack (Intrusion Detection Dataset):

Dataset: Intrusion Detection Dataset

Machine Learning Algorithm: Bayesian Belief Network achieved an accuracy of 99.16%.

The Bayesian Belief Network performed well in detecting this attack type.

MitMA Attack (Pooled Dataset):

Dataset: Pooled Dataset
Machine Learning Algorithm: Anomaly Detection achieved an "Outlier" value of 1.231.
The specific metric ("Outlier") is not described, making it unclear how well the algorithm performed.
DDoS Attack (Canadian Institute of Cybersecurity Dataset):
Dataset: Canadian Institute of Cybersecurity Dataset
Machine Learning Algorithms: SVM achieved an accuracy of 97.1%, Logistic Regression achieved 59.3%, and Decision Tree achieved 82.7%.
SVM outperformed the other two algorithms in this case.
DDoS Attack (Intrusion Detection System Generated Dataset):

Dataset: Intrusion Detection System Generated Dataset
Machine Learning Algorithms: SVM achieved an accuracy of 99.7%, NB achieved 98%, and Random Forest (RF) achieved 97.6%.
SVM and NB performed well, with SVM achieving the highest accuracy.
Malware Attack (Microsoft Malware Threat Prediction Kaggle):

Dataset: Microsoft Malware Threat Prediction Kaggle
Machine Learning Algorithm: Decision Tree achieved an accuracy of 83%.
Decision Tree performed with moderate accuracy for this type of attack.
SQL Injection Attack (Own Pooled Dataset):

Dataset: Own Pooled Dataset
Machine Learning Algorithms: AdaBoostClassifier achieved 99.3%, RandomForest achieved 99.80%, DecisionTree achieved 99.523%, TensorFlow Linear Classifier achieved 97.3%, TensorFlow Boosted Tree achieved 99.5%, Deep Artificial Neural Network (ANN) achieved 97.6%, Stochastic Gradient Descent (SGD) achieved 99.1% accuracy.
RandomForest, TensorFlow Boosted Tree, and DecisionTree seem to perform consistently well, with high accuracy percentages.
While comparing the performance of machine learning algorithms ,it varies significantly depending on the attack type, dataset quality, and algorithm choice. While some algorithms consistently perform well across multiple scenarios (such as SVM and RandomForest), others show varying levels of accuracy. Additionally, it's important to note that the specific metrics used to measure accuracy (e.g., "Outlier" value) and the absence of other metrics like precision, recall, and F1-score can impact the completeness of the evaluation.

SL No.	Cloud based Attack	Type of DataSet	Machine Learning Algorithms	Accuracy
1	Phishing	Email based	SVM	99.62
			NB	98

2	DDoS	CAIDA DATASET	Logistic Regression Navie BAyes	100%
3	MitMA	Intrusion Detection Dataset	Bayesian Belief N/w	99.16
4	MitMA	Pooled Dataset	Anomaly Detection	Outlier 1.231
5	DDOS	Dataset of Canadian institute of cybersecurity	SVM	97.1
			Logistic Regression	59.3
			Decision Tree	82.7
6	DDoS	Dataset generated with Intrusion Detection Sysytem	SVM	99.7
			NB	98
			RF	97.6
7	Malware Attack	Microsoft Malware threat prediction website Kaggle	DT	83%
8	SQL Injection	Own Pooled dataset	AdaBoostClassifier	99.3%,
			RandomForest,	99.80%,
			DecisionTree,	99.52%
			Tensorflow Linear classifier,	97.30%
			Tensorflow boosted tree	99.5%,
			Deep ANN	97.60%
			SGD	99.1%,

Conclusions

In this study, conducted a comprehensive analysis of machine learning algorithms applied to various cloud-based cybersecurity attack scenarios. The aim was to evaluate the effectiveness of different algorithms in detecting and mitigating such threats. Our findings reveal a diverse landscape of performance outcomes, highlighting the significance of algorithm selection and dataset characteristics.

It is observed that Support Vector Machine (SVM) consistently demonstrated high accuracy in multiple attack types, showcasing its robustness in detecting malicious activities. Decision Trees and Random Forest also exhibited commendable performance across different attack scenarios. Intriguingly, Logistic Regression and Naive Bayes presented varying degrees of accuracy, emphasizing the importance of algorithm choice based on attack characteristics.

The dataset's role in influencing algorithm performance cannot be understated. Datasets derived from reputable sources, such as the Canadian Institute of Cybersecurity and Microsoft Malware Threat Prediction Kaggle, contributed to reliable and consistent outcomes. However, careful consideration must be given to the quality and representativeness of datasets, as demonstrated by discrepancies in accuracy levels in certain cases.

This study underscores the need for a nuanced approach to algorithm selection, incorporating both attack-specific considerations and dataset quality assessment. Furthermore, we emphasize the importance of utilizing comprehensive evaluation metrics beyond accuracy, such as precision, recall, and F1-score, to provide a holistic perspective on algorithm performance.

In conclusion, this research sheds light on the intricate relationship between machine learning algorithms, datasets, and cybersecurity attack detection. By providing a comparative overview of performance outcomes, we contribute to the body of knowledge essential for enhancing the security posture of cloud-based systems. This study serves as a foundation for future research endeavors aimed at refining algorithmic approaches and advancing the domain of cloud-based cybersecurity.

Reference :

1. Umer Ahmed Butt1 · Rashid Amin1,2 · Hamza Aldabbas3 · Senthilkumar Mohan4 · Bader Alouffi5 · Ali Ahmadian , "Cloud-based email phishing attack using machine and deep learning algorithm" https://link.springer.com/article/10.1007/s40747-022-00760-3

2. Kimmi Kumari* and M. Mrunalini "Detecting Denial of Service attacks using machine learning algorithms", https://doi.org/10.1186/s40537-022-00616-0

3. EgwaliA.O1 , Alile S.O2 Department of Computer Science,Faculty of Physical Sciences,University of Benin, Benin City, Edo State, Nigeria.," Man-In-The-Middle Attack Detection Based on Bayesian Belief Network", International Journal of Academic Information Systems Research (IJAISR) ISSN: 2643-9026 Vol. 4, Issue 4, April – 2020,

4. Oliver Eigner,Fachhochschule Sankt Pölten | FH St. Pölten · Institute of IT Security Research Diplom," Paul Tavolato University of Vienna | UniWien · Fakultät für Informatik PhD," Detection of Man-in-the-Middle Attacks on Industrial Control Networks".

5. Md ABDUR RahmanAnhui University of Technology Ma'anshan, China," Detection of Distributed Denial of Service Attacks based on Machine Learning Algorithms". DOI:10.21742/IJSH.2020.14.2.02

6. Abdul Raoof Wani , Q.P. Rana , U. Saxena , Nitin Pandey,Amity University Noida, , Jamia Hamdard University,CCFISwanirauf@gmail.com,qprana@jamiahamdard.ac.in,Usaxena@akcds.in,Npandeyg@gmail.com"Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques"

7. Abel Yeboah-Ofori University of West London | UWL · School of Computing and Engineering "Classification of Malware Attacks Using Machine Learning In Decision Tree

8. Dharitri Tripathy, Rudrarajsinh Gohil, and Talal Halabi Applied Computer Science, University Of Winnipeg, Manitoba, Canada," Detecting SQL Injection Attacks in Cloud SaaS using Machine Learning" 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)

9. Mugunthan, S. R. (2019). Soft computing based autonomous low rate DDOS attack detection and security for cloud computing. J. Soft Comput. Paradig.(JSCP), 1(02), 80-90.
10. Dhanapal, A., & Nithyanandam, P. (2019). The slow HTTP distributed denial of service attack detection in the cloud. Scalable Computing: Practice and Experience, 20(2), 285-298.
11. Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 105, 102260.
12. Virupakshar, K. B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D. G. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Computer Science, 167, 2297-2307.
13. Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2021). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. Journal of Experimental & Theoretical Artificial Intelligence, 33(3), 405-424.
14. Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing, 10, 1985-1997.
15. Cheng, J., Li, M., Tang, X., Sheng, V. S., Liu, Y., & Guo, W. (2018). Flow correlation degree optimization driven random forest for detecting DDoS attacks in cloud computing. Security and Communication Networks, 2018, 1-14.
16. Idhammad, M., Afdel, K., & Belouch, M. (2018). Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. Security and Communication Networks, 2018.
17. Pandey, V. C., Peddoju, S. K., & Deshpande, P. S. (2018). A statistical and distributed packet filter against DDoS attacks in the Cloud environment. Sādhanā, 43, 1-9.
18. Kesavamoorthy, R., & Ruba Soundar, K. (2019). Swarm intelligence based autonomous DDoS attack detection and defense using a multi agent system. Cluster Computing, 22(Suppl 4), 9469-9476.
19. ALI BOU NASSIF 1 , MANAR ABU TALIB2 , QASSIM NASIR3 , HALAH ALBADANI 2 , AND FATIMA MOHAMAD DAKALBAB 2 “Machine Learning for Cloud Security: A Systematic Review” DOI: 10.1109/ACCESS.2021.3054129
20. Daniel Pop Institute e-Austria Timi¸soara Bd. Vasile Pˆarvan No. 4, 300223 Timi¸soara, Romˆania ,” Machine Learning and Cloud Computing: Survey of Distributed and SaaS Solutions” https://www.researchgate.net/publication/257068169
21. P. T. Jaeger, J. Lin, and J. M. Grimes, ‘‘Cloud computing and information policy: Computing in a policy cloud?’’ J. Inf. Technol. Politics, vol. 5, no. 3, pp. 269–283.
22. J. Wen, S. Li, Z. Lin, Y. Hu, and C. Huang, ‘‘Systematic literature review of machine learning based software development effort estimation models,’’ Inf. Softw. Technol., vol. 54, no. 1, pp. 41–59.
23. (ICSESS), Nov. 2017, pp. 712–717, doi: 10.1109/ICSESS.2017.8343013. [9] R. Moreno-Vozmediano, R. S. Montero, E. Huedo, and I. M. Llorente, ‘‘Efficient resource provisioning for elastic cloud services based on machine learning techniques,’’ J. Cloud Comput., vol. 8, no. 1, p. 5, Dec. 2019, doi: 10.1186/s13677-019-0128-9.