APPLICATIONS OF MACHINE LEARNING, DEEP LEARNING AND NEURAL NETWORKS IN CLOUD FORENSICS

Malluri Reddy Theertani
Student, Computer Science and Engineering , Vellore Institute of Technology , Vellore.
Vellore , India
theerthanimalluri@gmail.com

Neha Valeti
Student, Computer Science and Engineering, Vellore Institue of Tehnology,Vellore
Vellore, India
nehavaleti01@gmail.com

Darshini Solanki
Student, Computer Science and Engineering, Vellore Institute of Technology,Vellore
Vellore, India
darhsinisingh@gmail.com

Kakelli Anil Kumar
Associate Professor Sr. School of Computer Science Engineering
Vellore Institute of Technology, Vellore
Vellore, India
anilkumar.k@vit.ac.in

Abstract—— **Cloud computing has recently experienced rapid expansion, making it a major target for cybercrimes. Though cloud computing has many advantages, there are also substantial security issues related to confidentiality, integrity, privacy, and availability. Being a relatively new discipline, cloud forensics faces numerous challenges and issues with interpreting and analyzing data. Forensic investigators and law enforcement confront numerous difficulties in data collection, data protection, and evidence access. Several sophisticated models have been proposed in recent years aiming to accelerate the entire investigation process or address several issues that arise frequently in forensic investigations. This review paper seeks to comprehend the significance of various machine learning models which would help cloud forensics advance significantly. It also provides a detail information on cloud forensics as well as the research trends that have been going on in this field over the past few years. A detailed comparative analysis of different approaches of machine learning, deep learning, neural networks on development of cloud forensics has been presented in the paper.**

Keywords—cloud computing, cloud forensics, machine learning, deep learning, artificial neural networks

I. INTRODUCTION

Cloud computing has seen substantial change in the recent period. It is expected to be the most breakthrough technology ever developed [1]. Cloud computing has drastically transformed and changed the way IT resources are managed. Businesses are abandoning traditional methods of employing IT resources, in pursuit of cloud computing. Cloud computing, which offers quicker and more flexible resources, is simply the transmission of computing services through the internet, i.e., the cloud. Cloud computing is cost-effective since customers only pay for what they use. Under the pay-as-you-go concept, cloud computing assists organizations in lowering their operating expenses. Cloud computing is gaining popularity among businesses because it improves speed, efficiency, outcomes, reliability, and security [4]. Cloud computing is flexible and adaptive enough to enable remote data access and scalability as business requirements change [3].

Cloud computing protects huge volumes of privately owned data, which unavoidably contributes to the operation of cybercrime. Digital forensics on the cloud is gaining popularity as a result of numerous cybercrimes that are being committed there. By the official definition offered by NIST[1,5], digital forensics describes the application of technology to the identification, assessment, gathering, and analysis of information while safeguarding the data and keeping a precise chain of custody for such data. Cloud crime, as described by Ruan et al., is a crime that takes place in a cloud-based computing environment and uses the cloud as the object, subject, as well as tool of the crime [11].The term "cloud forensics" describes the application of digital forensics within cloud computing. Traditional approaches to forensic inquiry are less effective and successful due to decentralized data processing. Cloud forensics aids in overcoming the drawbacks of conventional methods [1]. Numerous problems and challenges are brought on by the emergence of cloud computing, notably in cloud forensics. Cloud forensics has advanced due to advancements in Big Data Analytics, Artificial Intelligence, and machine learning. The overall execution of cloud-based forensics seems complex, with several problems and difficulties involved at each level of cloud forensics, according to several studies undertaken by various academics [6].

In digital forensics, machine learning (ML) approaches can locate evidence more quickly than manual evaluation of enormous volumes of data produced from numerous sources. Investigators will therefore need to focus more on analyzing criminal dynamics and disclosure. Additionally, a range of digital criminal scenarios can benefit from the use of pattern-matching algorithms, anomaly detection tools, as well as other supervised and unsupervised ML models to enhance cyber forensics outcomes. Furthermore, deep learning algorithms may aid in locating intended evidence in unorganized data by creating connections and identifying other hidden patterns. Forensic investigators are using big data and Deep Learning (DL) approaches to solve this problem. Deep Neural Networks (DNN) have lately become successful at classification and recognition tasks. As a result, DNN systems with human-like accuracy on underlying data have gained wide acceptance and deployment.

In this review paper, we demonstrate various machine learning, deep learning, and neural network models applied in cloud forensics and show how they assist in simplifying and improving cloud forensics. The scope of this article will be on understanding how various machine learning, deep learning, and neural network models are employed in forensic investigations in the cloud.

II. CLOUD FORENSICS

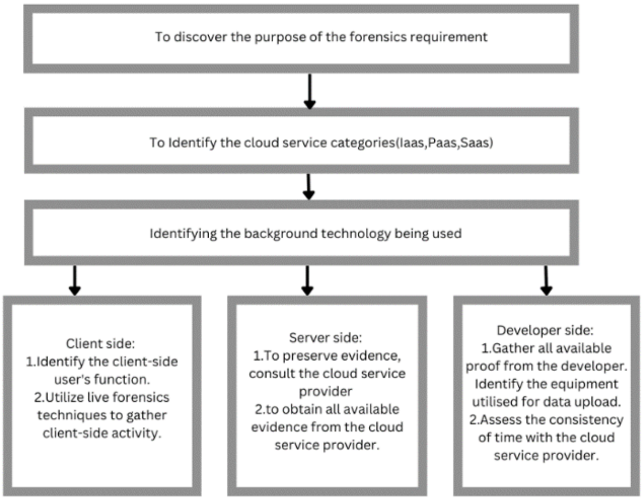
Cloud computing forensics is described as "the use of scientific principles, technological procedures as well as derived and proved methods to recreate previous cloud computing incidents through recognition, gathering, retention, investigation, explanation, and disclosure of digital evidence" [2] by the NIST. It takes a lot of computing power nowadays to interpret the data that these devices generate as digital technology is evolving so quickly. To enabling an investigator to completely focus on the investigative processes, the concept of a "Forensic Cloud" has been considered [15].

The definition of cloud forensics is "A method of cloud forensics is described as an examination of a cybercrime which requires proof or evidence obtained from any of the cloud-based platforms or cloud-based services" [2]. The number of crimes involving computers and web significantly increased over the past ten years, which has led to an equal rise in businesses that aim to help law enforcement by utilizing digital evidence to identify the offenders, techniques, casualties, and chronology of cyber-crimes. Digital forensics improved as a result, ensuring accurate presentation of data used as proof of criminality in court. However, as storage capacity outpaces network performance and latency advancements, forensic data is beginning to expand rapidly, making it more difficult to analyze them quickly [16]. We must use the forensics process provides the cloud examination since, as was previously said, cloud forensics would be a cross-disciplinary field of study including both cloud computing & digital forensics. Lack of physical access to computers presents new and disruptive issues for forensic experts in cloud forensics. Traditional methods of evidence gathering, and recovery no longer work due to the decentralized nature of data handling on the cloud. The technological features of digital forensics in a dispersed cloud setting are the main emphasis of this research [18].

A. PROCESS OF FORENSICS INVESTIGATION IN CLOUD:

The traditional computer forensics method consists of several processes; however, it may be roughly divided into the four essential phases- Collection, Examination, Analysis, and Reporting [19].The development of cloud computing has altered the forensic process's workflow today. In these virtual worlds where discs, storage, and network connections are shared and conventional ownership borders are blurred, we hardly have the power to physically acquire items. Very little study has been done to date on the condition of the tools, procedures, and approaches for obtaining legally acceptable forensic evidence in the cloud. The Forensics and Cloud Security Alliance experts concur that further study is required to create a framework of techniques and procedures that can withstand scrutiny in a court of law. They advise "having the ability to restore systems to past states, or even a necessity to go beyond 6-12 months for a recognized config." In order to enable the forensic monitoring of event logs while keeping in mind legal options and duties, corrective action might also be needed [20]. Basic forensic concepts and procedures apply when conducting forensic investigations in cloud settings, whether for retention, presentation in court, or the independent inquiry of employee misconduct.

Fig 1. Forensic Process broken down into four steps.


To discover the purpose of the forensics requirement
To Identify the cloud service categories(Iaas,Paas,Saas)
Identifying the background technology being used
Client side:
1.Identify the client-side user's function.
2.Utilize live forensics techniques to gather client-side activity.
Server side:
1.To preserve evidence, consult the cloud service provider
2.to obtain all available evidence from the cloud service provider.
Developer side:
1.Gather all available proof from the developer. Identify the equipment utilised for data upload.
2.Assess the consistency of time with the cloud service provider.

III. ML,NN,DL IN CLOUD FORENSICS

The priorities of modern man have fundamentally shifted because of digitization. Due to the sharp rise in cybercrimes, there is an increasing demand for digital forensics [25]. However, as of now, forensic analysis must cope with massive data [26]. Big data includes a huge amount of content. Additionally, with such a large amount of data, it's nearly impossible to manually do error-free analysis. Today's hottest technologies are artificial intelligence (AI) and machine learning (ML). Automation has been the way where everything is going. DF must thus advance with the digital age to analyze the data more effectively [27].

ML has gotten a lot of attention recently. It is a skill that is learned via practice and experience rather than through any sort of programming [28]. These algorithms must first be applied to a trained dataset. Online datasets are widely available for the use of ML in a variety of scientific domains. The selection of the algorithm is another crucial component of ML. Due to these decisions, ML can be divided into two categories. Unsupervised learning is the second and supervised learning is the first. We must train our well-labelled dataset for supervised learning. The training dataset for unsupervised learning must be unlabeled. Deep Learning is a sort of unsupervised learning that employs artificial neural networks at several degrees of hierarchy (ANN). The accuracy of machine learning (ML) relies upon the dataset and the algorithm. Many academics have looked into how well ML systems apply to DF. Malware analysis, network forensics, and mobile/memory forensics are the four key knowledge areas where it has primarily been used [27]. ML algorithms are typically run-on libraries and software tools. These software tools are fed datasets and the data gathered during the collecting phase of DF.

Fig 2. Research Trends in Cloud Forensics.

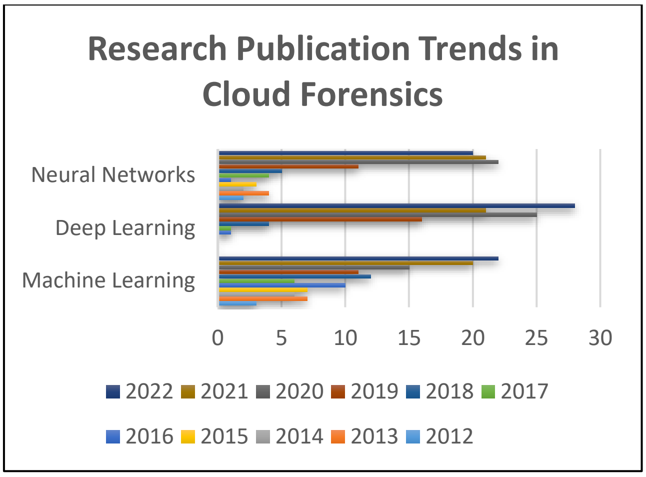


Fig 3. Research papers published on cloud forensics with machine learning.

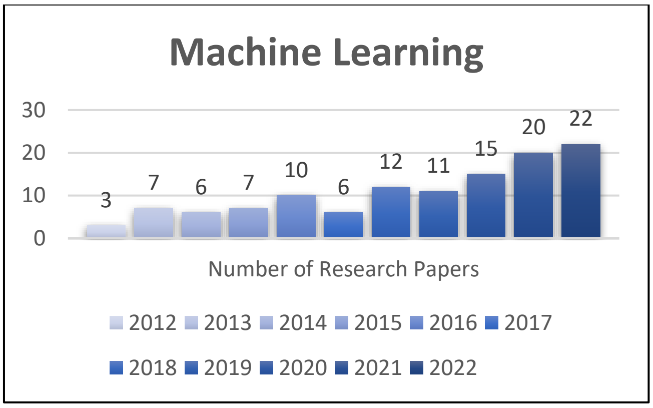


Fig 4. Research papers published on cloud forensics with deep learning.

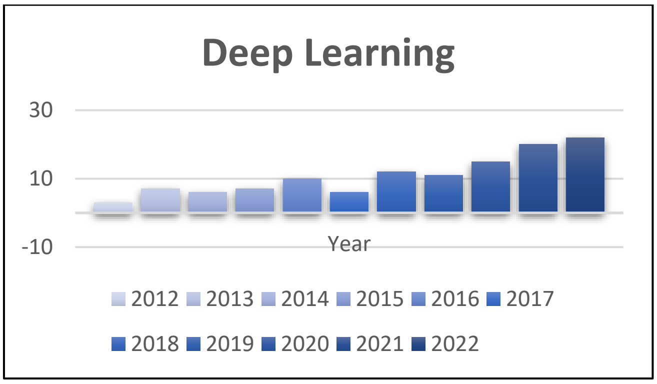
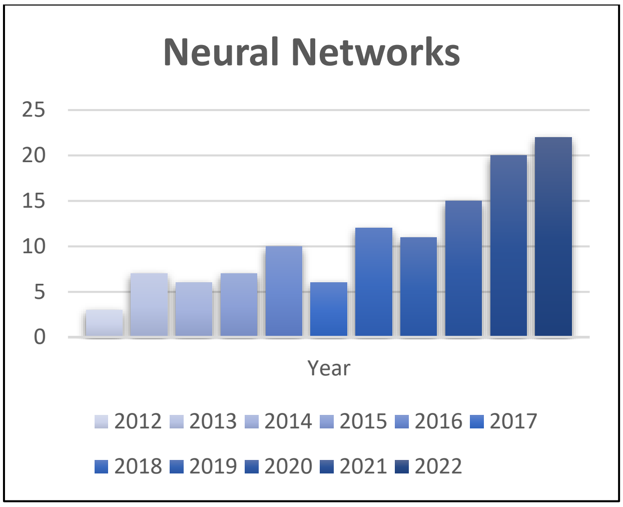


Fig 5. Research papers published on cloud forensics with neural networks.



IV. MACHINE LEARNING ALGORITHMS

Machine learning (ML) tactics are often flexible statistical methods for inferring conclusions or categorizing data. These methods are often explained by the algorithms which give specifics, although the predictions are made using the data and may produce a wider variety of predictors, also known as high-dimensional information [46]. Computers are programmed to use machine learning to optimize performance criteria based on prior knowledge [47]. There are three different ways to learn. A situation where the gained knowledge is to be deployed to the unseen necessitates supervised learning since such experience contains sensitive details that is missing [48]. Unsupervised education There are no labels on the data used as input or for training. By inferring pre-existing patterns or clusters from the datasets, a classifier is created. Both labelled and unlabeled data are present in the semi-supervised learning testing dataset. The classifiers undergo training to understand the patterns needed to classify, identify, and predict the data[49].

TABLE 1

S. No	**Most Common Machine Learning Algorithms**		
	Algorithm	***Strength***	***Weakness***
1	KNN	efficiency, competitive classification performance, and simplicity across numerous domains	poor run-time performances after a large training set.
2	DECISION TREE	Simple to grasp and might be used in conjunction with other decision-making processes.	Unstable
3	SVM	able to simulate nonlinear decision limits and resistant to overfitting.	They require a lot of memory and perform poorly with bigger datasets.

S. No	Most Common Machine Learning Algorithms		
	Algorithm	*Strength*	*Weakness*
4	RANDOM FOREST	use huge datasets effectively while maintaining accuracy.	Random forests are biased in favor of qualities with more levels when it comes to variables with no varied number of levels.
5	LINEAR REGRESSION	Simple to comprehend and explain, with the ability to be regularized to prevent overfitting.	when there are non-linear connections , performs badly. not adaptable enough to recognized intricate patterns
6	ANN	Processing in parallel and fault tolerance	The network's lifetime is unclear, and hardware reliance
7	DNN	simultaneous calculations and automated deduction features	big data volume, high training costs owing to complicated data models
8	K-MEAN	quick, easy, and adaptable	The number of clusters must be specified; however, it is challenging to do so.
9	C4.5	Handle properties that are both continuous and discrete	develops bare branches and is sensitive to noise

V. DATASETS USED IN DIGITAL FORENSICS(DF)

The accuracy of machine learning (ML) relies mostly on dataset as well as the algorithm. The ML Algorithms must first be applied to a training dataset. Online datasets are widely available for the use of ML in a variety of scientific domains. ML algorithms are often run on library resources and software tools. These software tools get fed datasets and the data gathered during the collecting phase of DF. It has been discovered from the examined publications that the dataset's correctness is highly crucial. However, it has been observed that various logical issues, including the choice of ML method and dataset type, have troubled researchers. Making the most efficient use of datasets is said to be the key difficulty in ML-based DF. Datasets are essential for precise outcomes [27].

TABLE 2.

S. No	Datasets Used in Various Fields		
	Source	*DF type*	*Samples*
1	Virus Share	Malware Analysis	Present it has 37,309,072 samples of malware
2	VX Heaven	Malware Analysis	271092 samples
3	Comodo Cloud Security Center	Malware Analysis	37,930 samples of malware
4	Pascal VOC 2012	Image Forensics	20 classes, roughly 6,929 segmentations in 11, 530 pictures, and 27, 450 objects
5	MS-COCO	Image Forensics	2,500,000 occurrences over 330 thousand photos, 80 different item types
6	IMDB-WIKI	Image Forensics	523,051 instances
7	Karina	Video Forensics	16 videos
8	Image Net	Image Forensics	14,197,122 instances
9	YFCC100M	Video Forensics	100 million
10	CAIDA	Network Forensics	33 datasets
11	Bot-IoT	Network Forensics	9543 benign + 73360900 instances of network attacks
12	Real Data Corpus	Memory Forensics	6748 GB Corpus
13	2007 INEX Wikipedia	Files/ Memory Forensics	75047 files

TABLE 3. Open-Source ML Tools

S. No	*Tool*	*Description*
1	WEKA	an open-source tool with a wide selection of ML algorithms.
2	Python WEKA Wrapper	a program that connects Python and WEKA libraries
3	RapidMiner	a machine learning and data mining tool
4	LIBSVM	Open-source C++ library that supports SVM for classification and regression analysis.
5	Dlib	ML toolkit in C++ that supports several algorithms

VI. RELATED WORK

S. Sachdeva, A. Ali, and others in [29] A new hybrid model was developed, using a genetic algorithm for the study of frequent patterns and the k-nearest neighbor method to maintain track of the KNN and MLP selection process. KNN and genetic algorithms are used in their strategy to improve the accuracy of attack classification. In comparison to the current ones, the accuracy of the suggested machine learning (KNN + MLP) algorithm was 99.93%. In this study, a prototype known as the trust surveillance system was used on the provided server. A variety of freeware cloud tools were also evaluated, along with a conservative forensic system on the client side, for possible evidence.

Saini, P. et al. [30] They used WEKA, a machine learning tool, to detect attacks in the data sources and applied different classifiers such as Naïve Bayes, Random Forest, MLP, and J48 (C4.5). The dataset used includes four types of attacks: UDP, HTTP floods, Smurf, and SIDDoS. To assess how well the classifiers were performing, they employed a confusion matrix. The computed accuracy for J48, MLP, Random Forest, and Naive Bayes were 98.64%, 98.63%, 98.10%, and 96.93%, respectively. The results show that J48 outperformed all 4 classifiers for calculating different classes, while Nave Bayes produced the worst results.

Patrascu A, and others in [31] They presented a novel solution that allows digital forensics investigators to supervise user behavior across a cloud platform and detect malicious actions in a reliable and secure manner. They utilized K-nearest neighbor (KNN), SVM classifier, and C4.5 decision tree. The results show that decision trees outperform SVM, KNN, and decision trees in terms of overall performance. Toshev et al. created a method centered upon Deep Neural Networks to classify images in [32], which was then used to object detection. They developed a multi-scale inference process that a few network applications can use to detect objects quickly and affordably at high resolution. The test set from the Pascal 2007 Visual Object Challenge (VOC) is the dataset that was used. The softmax classifier calculates the detection score. They have created a ground-breaking hybrid method based on data forensics, machine learning (ML), dynamic malware analysis, and cyber threat intelligence in [33]. Big data forensics is used to categorize linked zero-day attacks using behavioral analysis utilizing Decision Tree (DT) technique and estimate IP reputation at the pre-acceptance stage.

In [34] they sought to determine whether various machine learning (ML) methods might be used to track the activations of a historical file system to find increasing evidence. The training datasets have been gathered using VMware. Following data collection, the dataset was put into 7 different machine learning (ML) algorithms, including Feed Forward Neural Network (FFNN), Support Vector Machine (SVM), Random Forest (RF), Classification and Regression Trees (CART), and Naive Bayes (NB). Based on various evaluation metrics, the performance of these algorithms was compared. According to the experimental findings, NN and RF typically generated the best outcomes. In [35] they presented a two-tier architecture utilizing data mining and neural networks to identify a network-based intrusion. Through the use of two classifiers, they examined network behavior in their article that may be divided into misuse detection and anomaly detection. Utilizing hierarchical agglomerative clustering and an autonomous model on the training set, the input data was first categorized. The second step classified the input data using KNN as either regular traffic patterns or intrusions. They used the MLP algorithm for misuse detection and the reinforcement algorithm for anomaly identification. In their tests, the TP rate was 99% while the false positive rate was 1%.

In [36] They concentrated on the method of analyzing network security threats using machine learning algorithms and proposed Cloud-based Intelligent Security Technology (CIST) for tailored security service pro-visioning (unsupervised learning). The new-Kyoto 2006+ training dataset was utilized. SVM, Decision Tree, Neural Network, and Random Forest all performed less well than Random Forest.

Using a partitioned clustering technique, they provided a framework for collective anomaly detection in [37,38]. They validated their methods by comparing their results to those from other methodologies using benchmark data sets. They also ran into the issue of recognizing DoS assaults. They used experimental analysis to demonstrate that their methodology beat currently used clustering-based anomaly detection algorithms on the 1998 DARPA, 1999 KDD Cup, and Kyoto datasets.

In [39] This study focuses on DDoS attack detection and prevention. They used the Nave Bayes as well as Random Forest algorithms. The false percentage of pockets and the true percentage of packets were detected more efficiently by Nave Bayes than by random forest. They selected one cloud-based site to attack using the Parrot Sec Operating System. The analyzed data has been trained in the widely used but powerful tool 'WEKA'.

For locating the system's infection, [40] suggests using a potent combined Weighted Fuzzy K-means clustering and Auto Associative Neural Network (WFCM-AAN) malware detection approach. The proposed approach, which is based on evaluating and analyzing the performance metrics using graphical results, identifies malware with the highest precision of 92.45%, the highest recall of 75.48%, and the highest F measure of 58.47% when compared to the existing technique. They covered the two issues of anomaly and regular detection in this work. This approach will be used in future studies to detect numerous forms of attacks and boost the efficiency of malware detection.

Using VM snapshots, the authors Linda Joseph et al. [41] have suggested a method to identify malware from virtual machines. To categorize the VM snaps as attacked and non-attacked snapshots, machine learning techniques are used. Naive Bayes classifier as well as Random Forest were employed by the authors Amjad HB et al. [42] to regulate traffic on the network among cloud VMs.

In [43] A three-stage system for detecting cloud anti-forensic attacks is proposed known as the suspicious packets identification framework (SPIF). NSL-KDD is the dataset which is utilized. In this suggested approach, both signature analysis as well as anomaly detection across cloud levels are performed to classify the sort of attack which affected the packet. For performance evaluation, a variety of algorithms such as k-means, SVM, KNN, and Naive Bayes are utilized.

In [44] they proposed a generic digital forensic framework with a fusion algorithm for the cloud. The dataset that is used is NSL-KDD with ICMP Attacks, TCP Sync Attacks, and UDP Attacks. Various classifiers are utilized like MLP, Random Forest, and Naive Bayes. The total accuracy of MLP, Random Forest, and Naive Bayes were 98.6%, 98.02%, and 96.91%, respectively. The best retrieval and precision scores were obtained by MLP, with Naive Bayes performing the worst of the bunch.

TABLE 4.

Literature	***Objective***	***Type***	***Algorithms***	***Performance metrics***
[29]	Used to observe frequent pattern analysis in forensics	Supervised machine learning, Artificial neural network	k-nearest algorithm, KNN, MLP	99.93% accuracy
[30]	detect attacks in the data sources	Machine learning	Naïve Bayes, Random Forest, MLP, and J48 (C4.5)	J48 outperformed all 4 classifiers, while Nave Bayes produced the worst results.
[31]	supervise user behaviour across a cloud platform and detect malicious actions	Machine learning	utilized K-nearest neighbor (KNN), SVM classifier, and C4.5 decision tree	decision trees outperform SVM, KNN, and decision trees in terms of overall performance
[32]	Classify images/object detection	Deep Neural Networks	softmax classifier	---------
[33]	classify related zero-day attacks using behavioural analysis related	Machine learning	Decision Tree (DT) technique	----------
[34]	To track the activations of a historical file system to find increasing evidence	Machine learning	Forward Neural Network (FFNN), Support Vector Machine (SVM), Random Forest (RF), Classification and Regression Trees (CART), Naive Bayes (NB)	NN and RF typically generated the best outcomes
[35]	to identify a network-based intrusion	neural networks	KNN classification, MLP algorithm, reinforcement algorithm	a TP rate of 99% and a false positive rate of 1%.
[36]	proposed Cloud-based Intelligent Security Technology (CIST) for tailored security service provisioning	Unsupervised and supervised machine learning	SVM, Decision Tree, Neural Network, and Random Forest	Random Forest outperformed all others.
[39]	DDoS attack detection and prevention	Machine learning	Naive Bayes, Random Forest	Naïve bayes was more efficient than RF.
[40]	Malware detection method	ML, ANN	Weighted Fuzzy K-means clustering, and Auto Associative Neural Network (WFCM-AAN)	precision of 92.45%, the highest recall of 75.48%, and the highest F measure of 58.47%
[43]	A three-stage system for detecting cloud anti-forensic attacks	ML algorithms	k-means, SVM, KNN, and Naive Bayes are utilized.	Proposed RBNN+ k-means + Correlation shows high accuracy, while KNN+ k-means+ correlation shows least accuracy.

VII. CONCLUSION AND FUTIRE WORK

An integrated review for machine learning-based cloud forensics was built in this review study. Artificial neural networks and deep learning are mostly just two of the machine-learning techniques used in cloud forensics. Different datasets that are used are explained, and as data sizes grow, it is becoming increasingly challenging to conduct forensics on them. In this context, ML technology has demonstrated excellent outcomes. We have emphasized a number of academic papers that back ML-based cloud forensics. We have also presented the numbers of papers that were published in the recent years on cloud forensics through graphs. In all the papers, authors have used more than one type of machine learning, deep learning and artificial neural networks methods, they tested their efficiency and they found that the most popular algorithm among researchers, deep learning is considered to play a significant role in cloud forensics. Datasets play a crucial role for generating precise outcomes. An important concern in the overall ML-based cloud forensic process is how to use a dataset as efficiently as possible. In general, future improvements to the cloud forensics process will mostly concentrate on enhancing the effectiveness of the investigation process and more effectively integrating new technologies and approaches into the models.

REFERENCES

[1] Naaz, S., & Ahmad, F. (2016). Comparitive Study of Cloud Forensics Tools. *Communications on Applied Electronics*, *5*(3), 24–30. https://doi.org/10.5120/cae2016652258

[2] Purnaye, P., & Kulkarni, V. (2022). A Comprehensive Study of Cloud Forensics. *Archives of Computational Methods in Engineering*, *29*(1), 33–46. https://doi.org/10.1007/s11831-021-09575-w

[3] Alenezi, A., Zulkipli, N. H. N., Atlam, H. F., Walters, R. J., & Wills, G. B. (2017). The impact of cloud forensic readiness on security. *CLOSER 2017 - Proceedings of the 7th International Conference on Cloud Computing and Services Science*, 511–517. https://doi.org/10.5220/0006332705390545

[4] Zawoad, S. (n.d.). *SECURING THE CLOUD Digital Forensics in the Cloud*.

[5] Le-Khac, N.-A., & Scanlon, M. (2017). *Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service*. https://www.researchgate.net/publication/318981575

[6] Shahzad, F., Javed, A.R., Jalil, Z., Iqbal, F. (2022). Cyber Forensics with Machine Learning. In: Phung, D., Webb, G.I., Sammut, C. (eds) Encyclopedia of Machine Learning and Data Science. Springer, New York, NY. https://doi.org/10.1007/978-1-4899-7502-7_987-1

[7] Aditya, K., Grzonkowski, S., & Lekhac, N. (2018). Enabling Trust in Deep Learning Models: A Digital Forensics Case Study. Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE2018,1250–1255. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00172

[8] Sri Shakthi Institute of Engineering and Technology, Institute of Electrical and Electronics Engineers. Madras Section, All-India Council for Technical Education, & Institute of Electrical and Electronics Engineers. (n.d.). 2020 International Conference on Computer Communication and Informatics : January 22-24, 2020, Coimbatore, India.

[9] Shah, J. J., & Malik, L. G. (2013). Cloud forensics: Issues and challenges. International Conference on Emerging Trends in Engineering and Technology, ICETET, 138–139. https://doi.org/10.1109/ICETET.2013.44

[10] Aldawibi, O. O., Sharf, M. A., & Obaid, M. M. (2022). Cloud Computing Privacy: Concept , Issues And Solutions. 2022 IEEE Symposium on Industrial Electronics & Applications (ISIEA), 1–4. https://doi.org/10.1109/ISIEA54517.2022.9873688

[11] Zawoad, S. (n.d.). SECURING THE CLOUD Digital Forensics in the Cloud.

[12] Guo, H., Jin, B., & Shang, T. (2012). Forensic investigations in Cloud environments. Proceedings - 2012 International Conference on Computer Science and Information Processing, CSIP 2012, 248–251. https://doi.org/10.1109/CSIP.2012.6308841

[13] Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020, January). Cloud computing security issues & challenges: A review. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

[14] Agarwal, A., & Agarwal, A. (2011). The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences, 1(Special Issue on), 257-259.

[15] D. Svantesson, R. Clarke, "Privacy and Consumer Risks in Cloud Computing," Computer Law & Security Review, pp. 391-397, 2010.

[16] Vladimir Dobrosavljević, Mladen Veinović, Ivan Barać, "Standard Implementation in Cloud Forensics"Singidunum University, Danijelova 32, Belgrade, Serbia 2015.

[17] Dorey P.G., Leite A,"Commentary: Cloud computing –A security problem or solution?"Information Security Technical Report, 16 (3–4), pp. 89–96, Elsevier (2011)

[18] S. D. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments," Fifth International Conference on IT Security Incident Management and ITForensics,pp. 3-9, 2009.

[19] National Institute of Standards and Technology, "Guide to Interating Forensic Techniques into Incident Response", 2006

[20] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", December 2009, [1] http://en.wikipedia.org/wikilElectronic _identity_card, 2010.

[21] Scott Zimmerman and Dominick Glavach, "Cyber Forensics in the Cloud", IAnewsletter Vol 14 No 1, 2011.

[22] Sen, J., 2013. Security and Privacy Issues in Cloud Computing. Architectures and Protocols for Secure Information Technology, (iv), p.42.

[23] Chou, T., 2013. Security Threats on Cloud Computing Vulnerabilities. International Journal of Computer Science and Information Technology, 5(3), pp.79–88.

[24] Chouhan, P. & Singh, R., 2016. Security Attacks on Cloud Computing With Possible Solution. International Journal of Advanced Research in Computer Science and Software Engineering, 6(1), pp.92–96.

[25] S. Iqbal and S. A. Alharbi, "Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics". Digital Forensic Science, 2020

[26] G. S. Chhabra, V. P. Singh and M. Singh, "Cyber forensics framework for big data analytics in IoT environment using machine learning",Multimedia Tools Appl., pp. 1-20, Jul. 2018,

[27] Qadir, S., & Noor, B. (2021, May 20). Applications of Machine Learning in Digital Forensics. 2021 International Conference on Digital Futures and Transformative Technologies, ICoDT2 2021. https://doi.org/10.1109/ICoDT252288.2021.9441543

[28] S. Iqbal and S. A. Alharbi, "Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics". Digital Forensic Science, 2020

[29] Sachdeva, S., & Ali, A. (2021). A Hybrid approach using digital forensics for attack detection in a cloud network environment. In International Journal of Future Generation Communication and Networking (Vol. 14, Issue 1).

[30] Institute of Electrical and Electronics Engineers, Institute of Electrical and Electronics Engineers. Delhi Section, & INDIAcom (Conference) (14th: 2020 : New Delhi, I. (n.d.). 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom).

[31] Patrascu, A., Velciu, M. A., & Patriciu, V. V. (2015). Cloud computing digital forensics framework for automated anomalies detection. SACI 2015 - 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings, 505–510. https://doi.org/10.1109/SACI.2015.7208257

[32] C. Szegedy, A. Toshev and D. Erhan, "Deep neural networks for object detection",Proc. Adv. Neural Inf. Process. Syst., 2013.

[33] N. Usman, S. Usman, F. Khan, M.A. Jan, A. Sajid, M. Alazab, P. Watters, "Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics", Future Generation Computer Systems, Volume 118, 2021, Pp 124-141

[34] R. M. Mohammad and M. Alqahtani, "A comparison of machine learning techniques for file system forensics analysis",Journal of Information Security and Applications, vol. 46, no. 1, pp. 53-61, 2019.

[35] Divyatmika, Sreekesh, Manasa: Two-tier network anomaly detection model: a machine learning approach. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 42–47 (2016)

[36] Kim, H., Kim, J., Kim, Y., Kim, I., & Kim, K. J. (2019). Design of network threat detection and classification based on machine learning on cloud computing. Cluster Computing, 22, 2341–2350. https://doi.org/10.1007/s10586-018-1841-8

[37] Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. 60, 19–31 (2016)

[38] Ahmed, M., Mahmood, A.N.: Novel Approach for Network Traffic Pattern Analysis using Clustering based Collective Anomaly Detection, pp. 111–130. Springer, Berlin (2015). https://doi.org/10.1007/s40745-015-0035-Y

[39] Amjad, A., Alyas, T., Farooq, U., & Tariq, M. A. (2019). Detection and Mitigation of DDoS Attack in Cloud Computing Using Machine Learning Algorithm. EAI Endorsed Transactions on Scalable Information Systems, 6(23), 1–8. https://doi.org/10.4108/eai.29-7-2019.159834

[40] Yadav, R. M. (2019). Effective analysis of malware detection in cloud computing. Computers and Security, 83, 14–21. https://doi.org/10.1016/j.cose.2018.12.005

[41] Joseph L, Mukesh R (Sep 2018) Detection of malware attacks on virtual Machines for a Self-Heal Approach in cloud computing using VM snapshots. J Commun Software Syst 14(3):249–257

[42] Amjad HB, Sabyasachi P, Debasish J (2013) Machine learning approach for intrusion detection on cloud virtual machines. Int JAppl Innov Eng Manag 2(6):57–66

[43] Radha Rani, D., & Geethakumari, G. (2083). A framework for the identification of suspicious packets to detect anti-forensic attacks in the cloud environment. https://doi.org/10.1007/s12083-020-00975-6/Published

[44] Sachdeva, S., & Ali, A. (2022). Machine learning with digital forensics for attack classification in cloud network environment. International Journal of System Assurance Engineering and Management, 13, 156–165. https://doi.org/10.1007/s13198-021-01323-4

[45] B. Patel, Prof. H., & Kansara, Prof. N. (2021). Cloud Computing Deployment Models: A Comparative Study. International Journal of Innovative Research in Computer Science & Technology, 9(2), 45–50. https://doi.org/10.21276/ijircst.2021.9.2.8

[46] D. Buskirk, A. Kirchner, A. Eck, and C. S. Signorino, "An Introduction to Machine Learning Methods for Survey Researchers what are machine learning methods ?," pp. 0–3, 2018, doi: 10.29115/SP-2018-0004.

[47] E. Alpaydın, Introduction to Machine Learning Second Edition. .

[48] Ben-david, Understanding Machine Learning : From Theory to Algorithms. 2014.

[49] Das and R. N. Behera, "A Survey on Machine Learning : Concept ," pp. 1301–1309, 2017, doi: 10.15680/IJIRCCE.2017.

[50] Makkawi, A. M., & Yousif, A. (2021, February 26). Machine Learning for Cloud DDoS Attack Detection: A Systematic Review. Proceedings of: 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering, ICCCEEE 2020. https://doi.org/10.1109/ICCCEEE49695.2021.9429678