

Machine Learning Algorithms for Cloud Security

Douglas Allswell Kelechi

Department of Computer Science, School of Information and
Communication Tehnology, Federal University of Tehnology

Ituma Chinagolum

Department of Computer Science
Faculty of Science, Ebonyi State University, Abakaliki

Ukabuiro Ikenna Kelechi

Department of Computer Science
Faculty of Science, Abia State University, Uturu

Chinwe G Onukwugha

Department of Computer Science, School of Information and
Communication Tehnology, Federal University of Tehnology

Onwubiko Davidson Chisom

Department of Computer Science
Faculty of Science, Abia State University, Uturu

Dimoji Chigozie

Department of Computer Science, School of Information and
Communication Tehnology, Federal University of Tehnology

ABSTRACT

Any cloud data storage model's main goal is to make data accessible without sacrificing its security. Any model of cloud data storage that aims to ensure safety and effectiveness must take security into account. This research offers a secure model for cloud-based data protection. The suggested model offers a solution to the security problems that the cloud faces, including protection of data from infringements and defense against users with fictitious authorizations which have a negative impact on cloud security. The advantages and efficiency of security in cloud computing are provided by our suggested paradigm, which also improves cloud data encryption. It offers users of cloud computing security and scalability of data exchange. Our architecture satisfies the security requirements for cloud computing, including encryption, authorization, identification and authentication. Additionally, this architecture guards the system against any fictitious data owner who enters dangerous data that could undermine the primary objective of cloud services.

Keywords: Machine learning, Algorithm, Security, Cloud Computing, Storage and

INTRODUCTION

With the way we live being changed by information technology, our collection of digital data has begun to grow swiftly. Huge amounts of data are produced today in the commercial, research, manufacturing, and personal life sectors. Cloud computing, a rapidly evolving computing paradigm, enables users to share resources and data from a pool of dispersed computers supplied as a service via the Internet.

Without the direct involvement of the user, computer network services are made available through cloud computing, especially for data storage and processing capacity. In order to access and store data on a distant server, cloud computing applications are utilized (Isma et.al, 2021). Ninny & Shaveta (2017) assert that the use of the internet, cellphones, social media, refined ubiquitous computing, and many other technological advancements is the cause of the world's rising data volume.

There are many benefits to using cloud storage over older, more conventional storage solutions, especially in terms of scalability, cost savings, portability, and feature requirements. As more companies embrace cloud computing, this has led to attackers using it to obtain unauthorized access to the crucial data stored there. As a result of the shift from on-premises computing to the cloud, both customers and service providers now have a variety of security problems. In order to deliver a range of services via the Internet, reputable cloud service providers employ a number of different technologies, which introduces a number of security vulnerabilities.

According to Palumbo, et.al, (2019), the cloud model encourages and supports large applications of hardware and infrastructure (for providing the supported service). Despite its advantages, cloud computing has challenges as a cutting-edge computing model. Not every form of cloud deployment method will be advantageous for every service, every provider customer, or every stakeholder involved (Hussein & Khalid, 2017).

The problems related to cloud computing are addressed using a variety of techniques, including RSA, Blowfish, Advanced Encryption El Gamal encryption, machine learning, etc. Therefore, a detailed examination of the Machine Learning technique utilized to solve, recognize, or avoid Cloud security problems is the main goal of this work.

Machine Learning

The study of the algorithms and statistical models that computer systems employ to complete a task without being explicitly instructed is known as machine learning (ML). Due to the convergence of computer science and statistics as well as the foundations of artificial intelligence (AI) and data science, it is currently one of the technical domains with the fastest rates of progress.

Machine learning, a subset of Artificial Intelligence, computers can learn without being trained. Machine learning seeks to improve computer performance by learning from experience. Over time, it enables computers to respond to problems more successfully. Future problems that are comparable to this one can be solved by using this approach.

As defined by Arthur (2017), machine learning is learning from the past rather than through programming. When trained on a massive amount of historical data, machine learning models may predict the outcome of future events using a variety of techniques. It is typically thought of as a subset of artificial intelligence, which is frequently defined as a machine's capacity to replicate intelligent human behavior.

The algorithms that are used to train the models are the essential building blocks of machine learning. The type of machine learning technique that should be applied depends on the problem that has to be solved. In order to use machine learning to address an issue, data collecting must come first. Following that, the model is trained, tested, and deployed for actual use (Butt et.al, 2020; Sarker, 2021). The three main subcategories of machine learning are reinforcement learning, unsupervised learning, and supervised learning.

Future results are predicted using supervised machine learning techniques. Algorithms for supervised machine learning are primarily responsible for examining input data and classifying it appropriately. Only training utilizing a sizable amount of accurately labeled dataset with well-defined classes will allow for this class allocation to be done.

The main goal of supervised learning is to create a model from training or labeled data that will allow us to predict the behavior of new data. One can further categorize supervised learning into two different sorts of tasks: classification tasks, where the output is anticipated to be a categorical value, and regression tasks, where the outcome is anticipated to be a continuous value.

ML models are trained using unlabeled, uncategorized datasets in unsupervised machine learning techniques. Unsupervised machine learning algorithms independently find and learn all the data insights, such as data patterns, classifications, and categories, by examining the enormous dataset. The two types of unsupervised machine learning are clustering and association.

Semi-supervised learning, which utilizes both labeled and unlabeled data, combines the supervised and unsupervised techniques previously addressed. In light of this, this form of mechanism lies somewhere in the middle between learning "with supervision" and learning "without supervision." Semi-supervised learning is beneficial in a variety of situations where there are few labeled data sets and a large amount of unlabeled data in the actual world (Van et.al, 2020; Zhou and Zhou, 2021).

Predictions made using only the labeled data from the model are inferior to those made using a semi supervised learning model, which is the main goal of the technique. A method like this is often used in the detection of fraud, machine translation, and text classification.

Reinforcement learning is a class of machine learning technique that usually employs iterative learning to automatically examine the most successful behavior in a given environment. Kaelbling et al. (1996; Buconiu et al. (2010)) claim that reward learning happens gradually. The ultimate aim of this sort of learning, which is focused on benefits or costs, is to use the knowledge acquired from environmental activists to take actions that would either improve

benefits or decrease costs. To address basic or straightforward issues is not advised, nevertheless (Mohammed et al., 2016; Pugliese et al., 2021; Sarker, 2021). It is a powerful technique for developing AI models that may enhance the effectiveness of complex systems, such as supply and production networks, autonomous cars, and robotics.

Reinforcement learning's goal is to develop a system whose performance increases as a result of interactions with the environment. Even while this approach is quite similar to supervised learning, it also involves rewards and sanctions. Without having any prior understanding of the subject, unsupervised learning is the process of gleaning relevant information from unlabeled data. Clustering is one of the unsupervised learning strategies.

Machine learning approaches are used to handle data more efficiently and address security issues (Le et.al, 2019). Machine learning, as defined by Li et.al, (2013), is the application of artificial intelligence that allows frameworks to automatically learn new information and advance without being manually updated. The primary objective of the area is to create computer systems that can use machine learning to learn independently and at an appropriate pace.

Advantages of Machine Learning

Cognitive Computing:

By combining the principles of artificial intelligence and signal processing, cognitive computing is a novel technology that imitates human behavior. A machine-learning algorithm is trained in cognitive computing using a large amount of data. Cognitive clouds—made possible by fusing cloud and machine learning technology - allow users to access applications for cognitive computing.

Without interacting with humans, Cognitive Cloud is viewed as a self-learning process that completes activities resembling those carried out by humans. It employs a range of machine learning techniques, such as neural networks, pattern recognition, natural language processing, data mining, etc., to carry out actions that are similar to those carried out by humans. It can be applied to a wide range of industries, including banking and finance, retail, logistics, electricity and energy, cyber security, healthcare, and education.

Business intelligence:

Making better decisions is the core objective of business intelligence. Understand, organize, and enhance automated decision-making processes, such as those brought about by machine learning, using business intelligence. Business intelligence becomes essential for storing raw data as a result of the large amount of data utilized in cloud computing to train machine learning models. This unstructured data is also transformed into a structured format by using techniques for modification, transformation, and classification.

Internet of Things (IoT):

Cloud services, such as online data processing and archiving, are offered via the Internet of Things (IoT), a platform. Recently, cloud-based ML models have become more and more popular. It starts by asking for input data from the client, then uses cloud servers to run machine learning algorithms leveraging artificial neural networks (ANN), before sending output back to

the client. This raises privacy issues and discourages customers from using the services because the server might be holding sensitive client data.

Utilizing cloud computing is the simplest method for processing huge data packages produced by the Internet of Things. The majority of the time, it is used in real-time project environments as an event processing engine. It worked as a group effort, worked as a storehouse for Internet of Things data, and permitted remote access. For instance, when the Internet of Things is combined with personal devices, it can retrieve the status of your bus and train reservations and rebook these tickets for passengers whose trains were canceled or delayed.

Machine learning techniques are used to better manage data while also addressing security issues. Machine learning, according to Li et.al, (2013), is the application of artificial intelligence that enables frameworks to automatically take in new information and advance without being consciously updated. The main objective of the field is to develop software that can utilize machine learning to learn on its own and at the right pace (Callara & Wira, 2018).

Personal Assistant:

Nowadays, expanding a business requires having a personal virtual assistant that can assist clients just like a real person. Currently, a wide range of tasks are being carried out by these chatbots or personal virtual assistants in a number of industries, such as infrastructure, banking, healthcare, and education.

By using some frequently asked questions, even though they are still in the development stage and could use improvement, chatbots, which are becoming more and more popular, can handle common client problems more easily.

MACHINE LEARNING ALGORITHMS FOR CLOUD SECURITY

ML algorithms for cloud security include some of the following examples:

Artificial Neural Networks

Neural networks, according to an et.al, (2018), are among the best machine learning algorithms for simulating the human brain and its supporting communication network. It carries out its functions by emulating a biological creature's nervous system. A single neuron is the fundamental component of the nervous system. A number of interconnected layers of neurons make up the nervous system. According to an et.al, (2018), these pseudo-neurons help in classification, pattern recognition, and data mining.

These algorithms, according to Fei et.al, (2019), can shed light on intricate connections between the input set's components. The multilayer perceptron (MLP), which uses a nonparametric estimator, is another ANN version. Convolutional Neural Networks (CNN) are built on the foundation of translational invariance. In other words, the output function's value doesn't change while the input function is translated. To put it another way, the CNN will be able to determine the input's class even if it is translated.

Decision Trees and Random Forests

The class of algorithms that follow rankings includes these ones. The ranking technique is applied using a tree-like structure. Decision points are shown as nodes, while expected results are shown as leaves. The specific, specified attribute serves as the foundation for the leaf topology. A major benefit of these algorithms is that they are easy to read and understand (Fei et.al, 2019).

Bayesian Networks

In order to simulate the behavior of the system, these networks use conditional probability (Dhillon et.al, 2020). These networks use statistical methods to explain how distinct constituents' probabilities relate to one another. Based on the fact that the required event has already occurred, Bayesian networks show the likelihood that the subsequent event will also occur (Dhillon et.al, 2020). The approach is applicable to directed acyclic graphs.

According to Fei et.al, (2019), nodes stand in for random variables, and directed vertices represent impacts. In uncertain domain modeling, this machine learning approach excels (Fei et.al, 2019). Both supervised and unsupervised learning domains can benefit from its utilization (Fei et.al, 2019)

Support Vector Machines (SVMs)

These machines follow the boundary consideration theory in their operation. These supervised learning models create a hyperplane with the widest possible buffer between the data points to categorize the data into different groups. These devices are scalable and can be cascaded to do multilevel categorization. Because of their versatility, these SVMs have been enhanced to address regression concerns (Fei et.al, 2019).

Evolutionary Computations and Genetic Algorithms

These techniques for machine learning are based on concepts of biological evolution. According to Fei et.al, (2019), the guiding premise is "survival of the fittest." Trial and error is used in this situation to gradually learn under the guidance of the fitness function. The fitness function assesses the output's reliability or quality. The fitness function incorporates natural selection, mutation, and cross-over principles. According to Fei et.al, (2019), this approach can be utilized for reinforcement learning that is both supervised and unsupervised.

CHALLENGES TO CLOUD COMPUTING

Data protection, honesty, availability, authentication, and secrecy, as well as a lack of resources and skills, are among the most important security issues with cloud computing. Build inventory, Use, Transfer, Archive, and Kill are the six stages of the data life cycle.

1. A cloud computing platform must ensure the security of the client data as well as the dependability of the application platform. An efficient solution is anticipated in order to acquire a high level of reliability when a large-scale system is encountered. The effectiveness and status of the resource nodes are also controlled by a dynamic network management system, and failing or ineffective nodes are dynamically relocated.
2. Resource Provisioning and Scheduling: As resources are dynamically deprecated and expanded in response to user requests, management systems and cloud platforms are faced with new difficulties. An efficient cloud resource provisioning method that

improves resource allocation and utilization, decreases response times, and provides robustness and fault tolerance characteristics is crucial for the provisioning of cloud resources.

3. It is exceedingly difficult to manage a cloud computing platform. One of the important topics of research is resource consolidation, which has attracted a lot of interest from the research community recently. It entails managing the mechanisms for successfully regulating the system's resources, dynamically allocating and scheduling various resources, and managing clients, their billing processes, and service agreements.
4. Fault Tolerance: In the event that any hardware or software fails, cloud services will continue to operate normally. It is a significant problem to maintain the entire system operating and without performance deterioration in the event that such components fail.
5. Privacy and Transparency: In every cloud computing system, the privacy and openness of user data and cloud services are absolutely essential. Data privacy is extremely important for building confidence in a cloud-based business, as users' data and all associated credentials are held in a virtual environment. Similar to this, it is crucial that all systems and infrastructure are virtualized and that cloud services are transparent. Customers must be made aware of how their data will be handled, kept, and sent by cloud service providers. The deployment of security and privacy measures, as well as internal rules and technology, are all crucial from the client's perspective, especially if the customer is a large enterprise.
6. Security: The biggest issue with cloud computing right now is definitely security. Data security, information security, data integrity, and confidentiality are just a few of the issues it addresses. When it comes to the deployment and adoption of cloud computing, security is one of the major obstacles and concerns.

The use of intrusion detection systems (IDSs), host-based antivirus software, and firewalls as standard security measures are unable to provide sufficient security for virtualized systems. Different hazards are produced by the virtualized environments' rapid risk transmission (Subramanian & Jeyaraj, 2018). The Cloud Security Alliance (CSA) has identified the top 12 dangers to the cloud, which are listed by Subramanian and Jeyaraj (Subramanian & Jeyaraj, 2018). These risks include denial-of-service (DoS) assaults, compromised credentials and broken authentication, and DoS attacks.

According to Kamara and Lauter (Kamara & Lauter, 2010), the use of public clouds can lead to a variety of dangers. The greatest dangers come from data integrity and confidentiality, which result in several but linked problems. The three primary components of the crypto-cloud architecture that the authors suggest are the cloud storage service provider, the data consumer, and the data authority (the user who is in possession of the relevant data).

CLOUD COMPUTING SECURITY THREATS AND ATTACKS

Cloud computing security is essential for defending the environment against hostile and unauthorized access as well as the use of services made available via the use of internet technologies (Tadapaneni, 2020). Utilizing cloud computing services can expose users to security concerns such as shared cloud computing services, internal and external threats,

inadequate backups, phishing and social engineering, service attacks, and system vulnerabilities.

Due to businesses' increasing reliance on cloud computing, it is now more important than ever to secure cloud-driven services with settings that can protect the data that is accessible online (Jathanna & Jagli 2017). The advent of cloud computing services has boosted customer dependability, tremendous scalability, and low cost of corporate expansion.

Large firms can now automate both their routine company needs and wants as well as create a simple means of control that is readily accessible over the internet thanks to cloud computing technologies. Despite these advantages, there are still threats trying to undermine the benefits of the Cloud. The following are some of these risks:

1. Denial of Service (DoS) attacks are a common threat to online computer services. A common component of DoS attacks is the injection of a massive, uncontrollable amount of ping connection requests emanating from diverse machines. The system often experiences a DoS when ping queries reach the limit of the cloud computing infrastructure's support (Srinivasan et al., 2019). These requests are utilized, according to Odun-Ayo & colleagues (2018), to offer customers cloud computing services for system usability, management, and engagement. To stop cyber risks and exploitations, these services must be adequately provided, managed, choreographed, and watched over. Businesses embracing cloud computing must implement appropriate encryption and protocol assignments in order to prevent hackers and data loss during conversations done via internet connections (Tahboub & Saleh 2014).
2. The consistency, truthfulness, and dependability of data throughout its lifecycle is referred to as data integrity. Unauthorized people shouldn't be able to access data that is being kept, used, or altered in any way. Offering cloud computing services like PaaS, SaaS, and IaaS requires maintaining data integrity.
3. The impact of natural catastrophes and availability might be disastrous for a business that only uses one system and doesn't have a backup server set up, possibly resulting in the unintentional loss of important data and information (Ujjwal et al., 2019).
4. The loss of a backup results in the loss of previously saved data, which has serious consequences for a business functioning in a cloud environment. Setting up additional standby backup servers in case of emergencies can prevent this (Jan and others, 2020).
5. Data Privacy & Protection represents the safety of both the data that has been stored and utilized offline as well as the data that has been hosted over the cloud. The organization must adhere to the legislation, fulfill the standards for data protection, and satisfy the requirements for encryption in order to prevent having to pay out a lot of money in the event of a data breach (Shankarwar & Pawar, 2015).
6. Another issue with cloud computing is malicious insiders, who can be created by staff members' carelessness and minor errors, offering attackers and exploiters a chance to infiltrate the system and get unauthorized access (Saxena et al., 2020). In cloud computing, bandwidth issues with the cloud provider's end and the beginning of the data transmission chain are bottlenecks. Due to the fact that cloud computing helps to create a diversified corporate network in a dynamic way, there may be a latency problem related to the number of hops required for data transfer (Ibidunmoye, 2016).

According to Bondada & Bhanu (2014), insider assaults pose the greatest threat to the Cloud and data breaches are the biggest problem. In order to enable authentication to the user, they offer a mechanism that examines user keystrokes utilizing a hot-based user profiling technique. The attacks' main objectives include stealing user intellectual property, taking advantage of holes and other potential weaknesses in the cloud system, and committing insider fraud.

LITERATURE REVIEW

Every system is susceptible to security issues brought on by assaults, mistakes, improper configuration, openings, and other weaknesses. The several facets of cloud computing can lead to security issues. Among the challenges include data concerns, privacy concerns, data confidentiality concerns, and other issues (Oberoi et.al, 2017; Popli and Madhvi, 2019).

In this context, some security issues in cloud computing continue to be a challenging issue. As more businesses adopt the technology, cloud computing is growing every day, but it also poses a variety of security challenges. Many firms are reluctant to move their crucial data to the cloud due to the risks involved. A number of specific risks to the security and privacy of cloud services are brought about by the use of virtual machines. The cloud provider is hesitant to add security monitoring or intrusion detection and prevention technology due to transparency difficulties (Grabosky & Peter, 2015).

Although cloud computing is seen as a substantial and positive advance in IT architecture, more security work is still required to decrease its drawbacks. Because the Cloud data centers handle a sizable amount of personal and business data, cloud security risks and vulnerabilities must be detected and prevented. Cloud infrastructure may be exploited since it makes use of virtualization methods and common Internet protocols.

The detection of assaults, both known and new, benefits greatly from machine learning techniques. According to Chand, Mishra, Krishna, Pilli, and Govil (2016), machine learning is a group of algorithms that can identify patterns in data and predict future outcomes. To improve prediction, computer science and statistics are merged through machine learning (Chand et.al, 2016).

Whenever new data is collected, a machine learning system that has learned from prior data can forecast the outcome by building prediction models. Because a larger data set enables the creation of a better model, the amount of data utilized to build the model has an impact on how exactly the outcome is predicted.

Machine learning methods for enhancing data security were studied by Bhamare et al. (2016). Since virtualized server farms are gaining popularity as a practical foundation and solution for significant corporate applications, the idea of distributed computing was covered (Li et.al, 2020). To address security risks and protection issues in distributed computing, the researchers used an assistance model (Purniema et.al, 2013). They looked at several configurations now in use, underlying dangers, and security issues related to distributed computing, as well as their benefits and drawbacks.

Machine learning solutions should protect organizational data across all cloud applications of a business in a holistic manner. Because it addresses security issues and manages data more skillfully, ML provides a highly responsive and automated security solution. The objective of ML is to create computer programs that can choose their own optimal learning rate (Butt et.al, 2020).

Khan et.al, (2019) talked about an algorithm to address security concerns and enhance how the cloud system operates. Due to the outsider's erratic ways of gathering, storing, and producing knowledge, there is still little interest in it. Artificial neural networks (ANNs) were used by the authors to order the jumbled data.

Machine learning strategies for a secure cloud were assessed by Khan, Fan, et.al, (2019). Since third companies store, maintain, and handle the data, the data owners continue to show no interest in doing so. Abuse could nevertheless happen. The data has undergone safe processing using SMC. Effective cloud data safety and management are priorities for cloud data owners. One of the key tools used in numerous fields is pattern matching. The encrypted data has been used to assess both the supervised and unsupervised learning approaches' efficacy. Unsupervised learning performs better than it when given similar knowledge, while supervised learning performs better.

Elzamly et.al, (2019) used an ANN algorithm to deal with security concerns. To address security challenges, a banking institution used the ANN algorithm. ANNs are employed to improve cognition, performance, and brain processes.

In a 2017 research publication, Salman, Bhamare, Erbad, Jain, Samaka & recommended employing machine learning to block different cloud attacks in a multi-cloud scenario using intrusion detection systems. This approach's proposed intrusion detection system makes use of supervised machine learning algorithms from random forest and linear regression. The main advantage of this approach, in addition to identifying cloud risks, is that it also ensures threat categorization through the use of a state-of-the-art step-by-step algorithm. Accuracy rates for threat detection and categorization are 99.0% and 93.6%, respectively.

METHODOLOGY

In accordance with the objectives of this study, in order to carry out a thorough, methodical literature review. We searched six research databases for the source data and located the relevant publications using the Systematic Literature Review technique, which seeks to summarize and clarify the Machine Learning (ML) techniques and implementations that were employed in Cloud security from 2004 to 2019 inclusive. These repositories were thoroughly investigated using various ML-related queries. The predefined queries returned a large number of research papers, but only the most relevant ones were kept for this review.

CONCLUSION AND FUTURE WORK

Currently, the biggest issue with cloud computing is security. Data security, information security, data integrity, and confidentiality are a few of the issues it covers. When it comes to the deployment and adoption of cloud computing, security is one of the main issues and concerns.

Due to its advantages of quick setup, easy access, large storage space, and affordability, cloud computing technology is quickly becoming more popular. The biggest impediment to the cloud computing paradigm's acceptance is the rise in security worries. As a result, both academics and experts in cloud security are very interested in security. Regarding safeguarding against threats, vulnerabilities, and assaults in the cloud, there is still a sizable security gap.

Despite the huge number of research projects that have been conducted in this field, there are, to the best of our knowledge, only few Systematic Reviews on cloud security applying machine learning. For our analysis, we carefully researched and selected research papers on the use of ML methods for cloud security and other security-related problems.

This study looked at the various safeguards against security intrusions in the virtualized cloud environment. To address the issues with cloud security, numerous machine learning security models have also been introduced in this work. Finally, the assessment of the research challenges and potential future paths in cloud security motivates the researchers to focus on developing security from that perspective.

In the future, we propose an intrusion detection system that will utilize an enhanced and optimized machine learning algorithm to give more precise cloud data security.

ACKNOWLEDGMENT

We would like to thank the reviewers who chose to remain anonymous for their constructive feedback, which considerably improved the quality of this study. The authors also thank NCS for funding this research.

References

- An, X., Zhou, X., Lü, X., Lin, F & Yang, L. (2018) "Sample Selected Extreme Learning Machine Based Intrusion Detection in Fog Computing and MEC," *Wireless Communications and Mobile Computing*, vol. vol. 2018, pp. 1-10, 2018.
- Arthur Samuel (2017). "Machine Learning." Wikipedia. Wikimedia Foundation, 01 Apr. 2017. Web. 04 Apr. 2017.
- Bhamare, D.; Salman, T.; Samaka, M.; Erbad, A. (2016). Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In *Proceedings of the International Conference on Information Science and Security*, Jaipur, India, 16–20 December 2016; pp. 1–5
- Bondada M. B & Bhanu, S. M. S. (2014) "Analyzing user behavior using keystroke dynamics to protect cloud from malicious insiders," in *Proc. IEEE Int. Conf. Cloud Comput. Emerg. Markets (CCEM)*, Oct. 2014, pp. 1–8, doi: 10.1109/CCEM.2014.7015481
- Butt U. A., Mehmood M., Shah S. B. H., Amin R., Shaukat M. W., Raza S. M., S. M. Suh S. M and Piran M. J (2020), A review of machine learning algorithms for cloud computing security," *Electronics*, vol. 9, no. 9, p. 1379, Aug. 2020, doi: 10.3390/electronics9091379
- Callara, M.& Wira, P. (2018) User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In *Proceedings of the 2018 International Conference on Applied Smart Systems*, Médéa, Algeria, 24–25 November 2018; pp. 1–6

Chand N, Mishra P, Krishna C. R, Pilli E. S & Govil M. C (2016) "A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection," in Proc. Int. Conf. Adv. Comput., Commun., Autom. (ICACCA) (Spring), Apr. 2016, pp. '1-6, doi: 10.1109/ICACCA.2016.7578859

Dhillon, A., Singh, A., Vohra, H., Ellis, C., Varghese, B & Gil, S. (2020) "IoT Pulse: machine learning-based enterprise health information system to predict alcohol addiction in Punjab (India) using IoT and fog computing," *Enterprise Information Systems*, pp. 1-34, 21 Sep 2020

Elzamy, A.; Hussin, B & Basari, A.S. (2019) Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study. *Int. J. Grid Distrib. Comput.* 2016, 9, 137–158. [CrossRef]

Fei, X., Shah, N., Verba, N., Chao, K.-M., Sanchez-Anguix, V., Lewandowski, J., James A & Usman, Z. (2019) "CPS data streams analytics based on machine learning for Cloud and Fog Computing: A survey," *Future Generation Computer Systems*, vol. Volume 90, pp. 435-450, 2019

Grabosky, Peter. "Organized cybercrime and national security." *Cybercrime Risks and Responses*. Palgrave Macmillan, London, 2015. 67-80

Hussein, N.H & Khalid, A. (2017) A survey of Cloud Computing Security challenges and solutions. *Int. J. Comput. Sci. Inf. Secur.* 2017, 1, 52–56.

Ibidunmoye, O. (2016). Performance problem diagnosis in cloud infrastructures (Doctoral dissertation, Department of Computing Science, Umeå University).

Isma Zulifqar, Sadia Anayat & Imtiaz Kharal, (2021), A Review of Data Security Challenges and their Solutions in Cloud Computing, *I.J. Information Engineering and Electronic Business*, 2021, 3, 30-38 Published Online June 2021 in MECS (<http://www.mecspress.org/>) DOI: 10.5815/ijieeb.2021.03.04

Jan, S. U., Ghani, D., Alshdadi, A., & Daud, A. (2020). Issues and challenges in cloud storage architecture: a survey. , *Issues and Challenges in Cloud Storage Architecture: A Survey*. Researchpedia Journal of Computing, Volume 1, Issue 1, Article 6, Pages 50–65, Jun 2020. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630761 accessed: May 07 2021

Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement learning: A survey. *Journal of artificial intelligence research*, 4(1), 237-285.

Kamara S & Lauter K, (2010) Cryptographic Cloud Storage,|| in *Financial Cryptography and Data Security*, Berlin, Heidelberg, 2010, pp. 136–149. doi: 10.1007/978-3-642-14992-4_13.

Khan, A.N.; Fan, M.Y; Malik, A. & Memon, R.A (2019). Learning from Privacy Preserved Encrypted Data on Cloud Through Supervised and Unsupervised Machine Learning. In *Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies*, Sindh, Pakistan, 29–30 January 2019; pp. 1–5.

Le Duc, T.; Leiva, R.G.; Casari, P.; Östberg, P.O. (2019) Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. *ACM Comput. Surv.* 2019, 52, 1–39. [CrossRef]

Li, K.; Gibson, C.; Ho, D.; Zhou, Q.; Kim, J.; Buhisi, O.; Gerber, M. (2013) Assessment of machine learning algorithms in cloud computing frameworks. In *Proceedings of the IEEE Systems and Information Engineering Design Symposium*, Charlottesville, VA, USA, 26 April 2013; pp. 98–103.

Li, C.; Song, M.; Zhang, M.; Luo, Y. (2020). Effective replica management for improving reliability and availability in edge-cloud computing environment. *J. Parallel Distrib. Comput.* 2020, 143, 107–128. [CrossRef]

Mohammed, M., Khan, M. B., & Bashier, E. B. M. (2016). *Machine learning: algorithms and applications*. CRC Press.

- Oberoi, Priya & Sumit Mittal. (2017). Survey of various security attacks in Clouds based Environments. *International Journal of Advanced Research in Computer Science* 8.9 (2017)
- Odun-Ayo, I., Geteloma, V., Falade, A., Oyom, P., & Toro-Abasi, W. (2019, December). A Systematic Mapping Study of Utility-Driven Models and Mechanisms for Interclouds or Federations. In *Journal of Physics: Conference Series* (Vol. 1378, No. 4, p. 042008). IOP Publishing.
- Palumbo, F.; Aceto, G.; Botta, A.; Ciuonzo, D.; Persico, V. & Pescapé, A. (2019) Characterizing Cloud-to-user Latency as perceived by AWS and Azure Users spread over the Globe. In *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, Taipei, Taiwan, 7–11 December 2019; pp. 1–6
- Popli, Madhvi. (2019) A Survey on Cloud Security Issues and Challenges, 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2019
- Pugliese, R., Regondi, S., & Marini, R. (2021). Machine learning-based approach: Global trends, research directions, and regulatory standpoints. *Data Science and Management*, 4, 19-29.
- Purniema, P.; Kannan, R. & Jaisankar, N. (2013) Security Threat and Attack in Cloud Infrastructure: A Survey. *Int. J. Comput. Sci. Appl.* 2013, 2, 1–12
- Sarker, I.H. (2021) Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN computer science* volume. 2, 3 (2021): 160.
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, 9(9), 1460.
- Shankarwar, M. U., & Pawar, A. V. (2015). Security and privacy in cloud computing: A survey. In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014* (pp. 1-11). Springer, Cham
- Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Kumar, A. D. (2019, February). A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In *Intelligent Communication Technologies and Virtual Mobile Networks* (pp. 252-270). Springer, Cham.
- Subramanian N & Jeyaraj A (2018) Recent security challenges in cloud computing, || *Comput. Electr. Eng.*, vol. 71, pp. 28–42, Oct. 2018, doi: 10.1016/j.compeleceng.2018.06.006.
- Tadapaneni, N. R. (2020). Cloud Computing Security Challenges. *International Journal of Innovations in Engineering Research and Technology*, 6(7) (pp. 1-6)
- Tahboub, R., & Saleh, Y. (2014, January). Data leakage/loss prevention systems (DLP). In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-6). IEEE.
- Ujjwal, K. C., Garg, S., Hilton, J., Aryal, J., & Forbes-Smith, N. (2019). Cloud Computing in natural hazard modeling systems: Current research trends and future directions. *International Journal of Disaster Risk Reduction*, 38, 101188.
- Van Engelen, J. E., & Hoos, H. H. (2020). A survey on semi-supervised learning. *Machine learning*, 109(2), 373-440.
- Zhou, Z. H., & Zhou, Z. H. (2021). Semi-supervised learning. *Machine Learning*, 315-341.