International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2024.8.10

Volume 10, Issue 8
August - 2024

Subject Review: Enhancing Cyber Security through Machine Learning Model in Cloud Computing Environment

Raniah Ali Mustafa[1], Haitham Salman Chyad[2], Dena Nadir George[3]

[1,2,3]Computer Science Department

College of Education

Mustansiriyah University

Baghdad, Iraq

ABSTRACT

Cloud computing (CC) has become more and more popular in environments that use distributed computing. Cloud-based processing and data storage is becoming a global trend. Perhaps might put up the effect that Software as a Service (SaaS) has on numerous commercial applications and daily lives as disruptive technology. Cloud computing (CC) is an extension of Internet-based computing, where devices can access shared software, resources, and data as required. Machine learning (ML) has become a popular tool in the area of cybersecurity (CS) through the cloud computing environment in recent years. Examples of its applications include biometric-based user authentication and the detection of malware or intrusions. However, attacks on machine learning (ML) algorithms may occur in both the testing and training phases, which typically results in significant performance reductions and safety breaches. This article provides a comprehensive study on the use of machine learning (ML) algorithms to enhance cybersecurity (CS), as well as a comparison of most of the machine learning (ML) techniques mentioned in the work. The article presents future work of previous works that help researchers find ways to improve cybersecurity.

Key Words: Attacks cyber (AC), Cyber Security (CS), Cloud computing (CC), Intrusion detection (ID), Machine learning (ML), Software as a Service (SaaS).

1. INTRODUCTION

Because cloud computing enables modern enterprises to access, store and analyse data accurately and efficiently[1], they have embraced it as a crucial component. But continued use of cloud computing also raises data security issues [2,3]. Therefore, to protect sensitive data from theft and unwanted access, cloud computing security must be improved. Experts have recognized machine learning (ML) as a potential approach to improve cloud computing security (CCS) [4]. Machine learning (ML) techniques are utilized to address data more efficiently and solve security-related problems [5]. Machine learning (ML) is the application of artificial intelligence (AI) which allows structures to learn and adapt naturally without the required for special customization [6]. Machine learning (ML) is concerned with expanding computer programs which can learn on their own at a suitable rate. In order to obtain patterns in data and subsequently make best decisions about the models presented, a learning strategy begins with perceptions or data, including models, guidance, or direct understanding [7]. In order to leverage security capabilities as attacks become increasingly sophisticated, the cybersecurity industry is leveraging cutting-edge technologies such as machine learning (ML). Detecting even the smallest malware or ransomware attack activity before it infiltrates the system is the aim of machine learning (ML) in cybersecurity (CS).

1.1 Benefits of Machine Learning (ML) in Cybersecurity (CS) [8,9]

There are many benefits to using machine learning (ML) to address cybersecurity (CS)-related problems. These comprise:

1. Synthesize huge amounts of data rapidly: One of their biggest problems is the analysis requirement to quickly gather intelligence from across the attack surface, often produced much faster than their teams can manually

assess. Machine learning can rapidly analyse large amounts (LA) of historical and dynamic intelligence, enabling teams to operationalize data from disparate sources in near real-time.

2. Expand expert intelligence by using long training cycles that let models learn for a changing population sample. This sample can include discoveries that have been classified by analysts or alerts that have been reviewed by analysts. Furthermore, it helps prevent the repeated generation of false positives by enabling models to comprehend and utilize expert-provided ground truth.
3. Automate laborious, manual tasks: Security teams can eliminate time-consuming, repetitive tasks by implementing machine learning to specific tasks. As a result, machines will be able to scale their response to incoming signals and allocate time and resources to complicated strategic initiatives.
4. Improve the productivity of analysts: By providing real-time, current intelligence to augment analyst expertise, machine learning can help threat and security analysts allocate resources more wisely to address their organization's most pressing vulnerabilities and investigate time-sensitive issues discovered using machine learning (ML) alerts.

1.2 Machine learning (ML) Challenges for Cybersecurity (CS) [9,10]

1. The first is the greatly increased standards for accuracy: For example, if you're just doing image processing and the system misidentifies a dog as a cat, it might be unpleasant, but it probably won't have a life-or-death consequence. If a machine learning system incorrectly classifies an invalid data packet for a valid one, it might have major consequences, such as initiating an attack on a hospital's devices.
2. The second difficulty is getting access to a large amount of training data, especially labeled data: To create more accurate models and predictions, machine learning (ML) requires the collection of a large amount of data. Obtaining malware samples is much more challenging than obtaining data for natural language processing (NLP) or image processing (IP). Attack information is scarce, and a large amount of important security risk information is unavailable because of privacy concerns.
3. The third difficulty is the fact of the matter: Unlike images, cybersecurity is not always available or constant. The cybersecurity landscape is dynamic and ever-changing. Since malware is a dynamic field, no single database can claim to contain all of the world's malware. What is the reality that we must take into account?
4. Lack of talent: We need to combine machine learning (ML) expertise with domain experience in order for machine learning (ML) to be relevant in any field. Finding experts in both machine learning (ML) and security is hard; many individuals are only proficient at one or the other. It is significant to ensure that machine learning (ML) data scientists and security professionals work together, despite the fact that they don't share the same language and use different approaches. They have to acquire cooperation skills. Effective use of machine learning (ML) in cybersecurity (CS) depends on these two groups.
5. Given the critical role that cybersecurity plays in every organization, it is absolutely imperative that we ensure that the machine learning we use for cybersecurity is secure in itself. As this topic has been a subject of academic study, we applaud and encourage commercial efforts to protect machine learning (ML) models and data. To ensure the security of our machine learning (ML), Palo Alto Networks is encouraging innovation and adopting the necessary safety measures.
6. The final challenge is the explainability of machine learning (ML) models. It is significant to understand the results of machine learning (ML) in order for us to act accordingly.

2. MACHINE LEARNING (ML) TECHNIQUES

The multiple types of machine learning (ML) techniques are summarized as follows [11]:

1. SML (Supervised Machine Learning): utilizing labeled databases (DB) to train models for predicting findings depend on the training provided is indicates as supervised machine learning (ML). In supervised learning, mapping an input variable to an output variable is the main goal. Furthermore, supervised machine learning (SML) is divided into two primary categories:
    - Classification: algorithms deal with issues related to classification and produce categorical outputs.

DOI: 10.31695/IJASRE.2024.8.10

- Regression: relationship among the I/O variables is linear.

2. UML (Unsupervised Machine Learning): Unsupervised learning (UL) involves utilize an unlabeled database (DB) to train the machine learning (ML) model, enabling it to predicting findings without individual supervision. Without individual assistance, the model learns from the data. UML (Unsupervised machine learning) models, unlike SL (supervised learning), are able to find patterns and insights on their own.
3. SSL (Semi-supervised learning): Due it trains models utilizing a large amount (LA) of unlabeled data and a small amount (SA) of labeled data, SML (semi-supervised machine learning) is among UML (unsupervised machine learning) and SML (supervised machine learning).
4. RL (Reinforcement learning): The basis of this machine learning (ML) training technique is the reinforcement of acceptable behaviors and punishing undesirable behaviors. A trained model has the ability to sense and understand its surroundings before acting and acquire new skills through trial and error. For RL (reinforcement learning), labeled data is not available, unlike SML (supervised machine learning).

The following figure (1) illustrates the primary categories of machine learning (ML) techniques along with some typical algorithms.

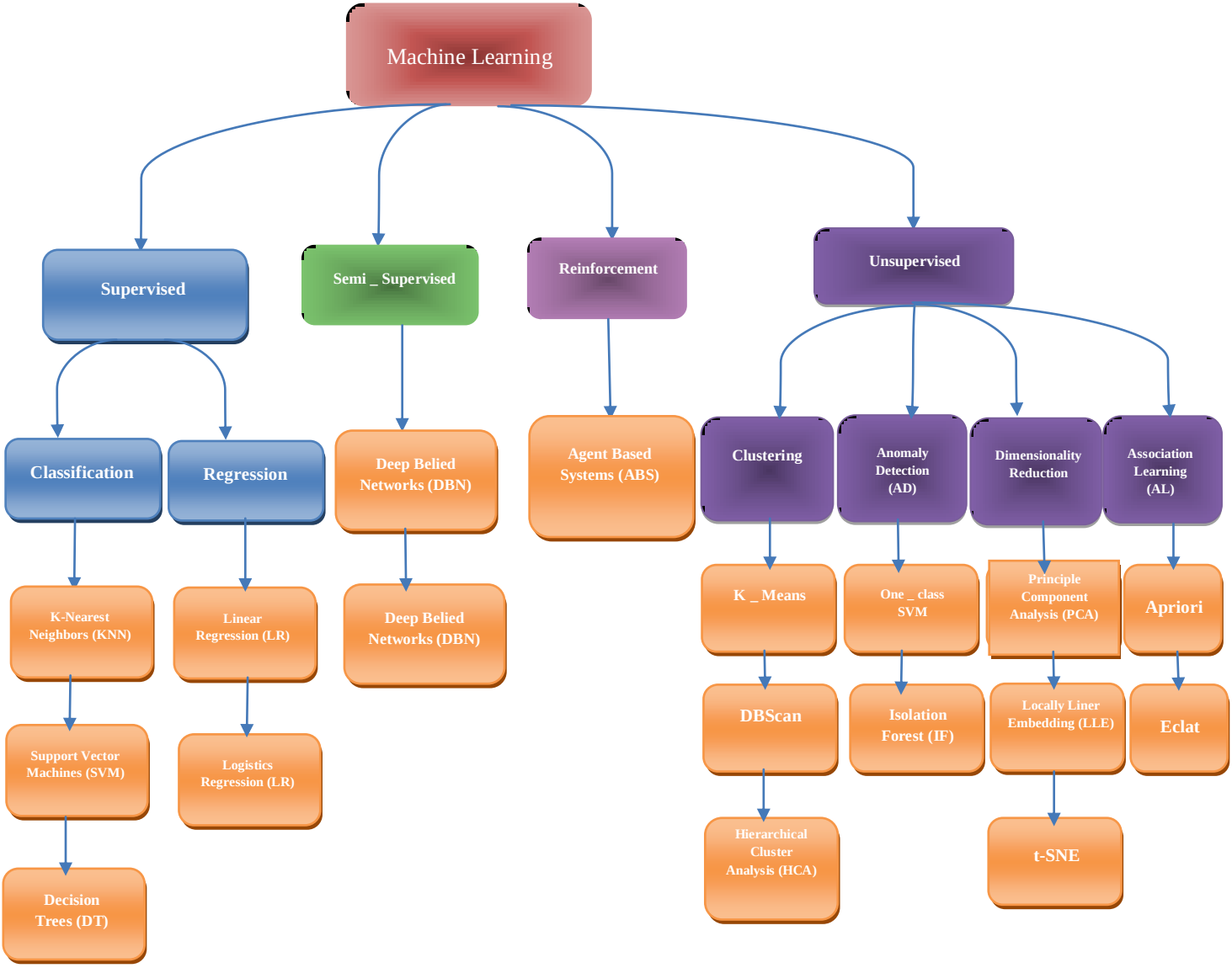

Fig.1 Show machine learning (ML) techniques along with some typical algorithms [12]

DOI: 10.31695/IJASRE.2024.8.10

3. MACHINE LEARNING (ML) IN CYBER SECURITY (CS)

Machine learning (ML) is a powerful tool that has applications in many different information security domains. Effective network intrusion detection systems and anti-phishing algorithms are available. The development of authentication systems, evaluation of protocol implementation efficiency, evaluation of the security of human interaction evidence, classification of smart meter data, and other related tasks can be accomplished effectively using machine learning (ML) [13].

The cyber security (CS) industry has seen a tremendous deal of opportunity from machine learning (ML). Because they can handle more computational processing, new machine learning (ML) models can significantly increase the precision of the detection of threats and improve network visibility. They are also ushering in a new era of autonomous reaction, where a machine scheme becomes clever enough to know when and how to retaliate against already initiated threats. The application of various machine learning (ML) techniques has effectively addressed numerous computer security issues [14].

Over the previous few years, machine learning (ML) techniques have been successfully utilized in a wide range of cybersecurity problems across a wide range of application areas. Shown in fig. 2, a wide range of other applications have also become popular, including cyberbullying detection (CBD), malware analysis (MA) and detection, fraud detection (FD) and anomaly detection (AD), IoT attacks, zero-day attack detection, threat analysis (TA), and intrusion detection (ID), spam filtering (SF).

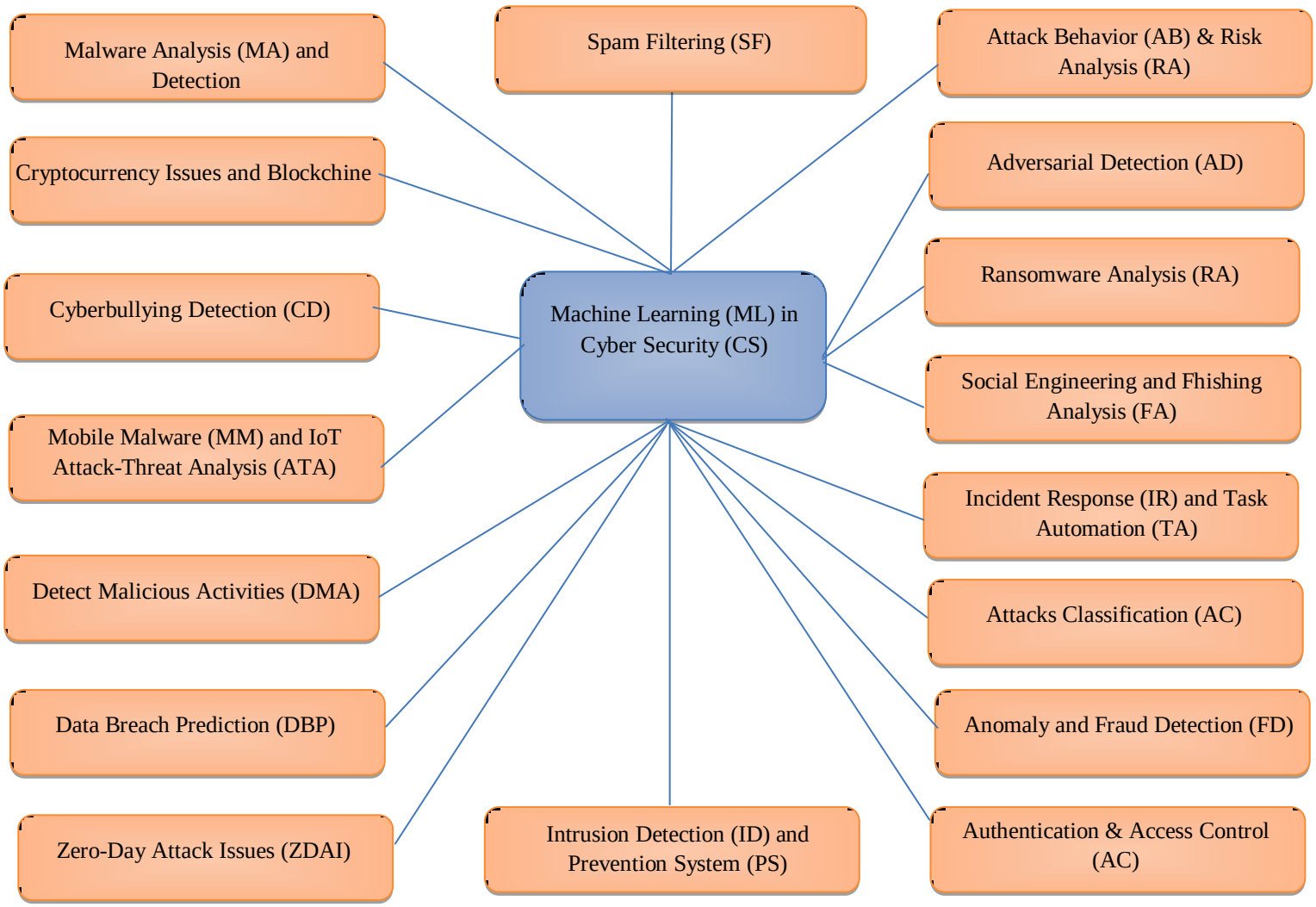

Fig 2. Cybersecurity (CS) applications for Machine Learning (ML) [15]

DOI: 10.31695/IJASRE.2024.8.10

4. PERVIOUS WORKS

In the past, machine learning (ML) technology has been used in several ways to enhance cybersecurity (CS). A study was conducted on detecting and preventing insider threats in cloud computing utilizing machine learning (ML) models. Z. Abbas and S. Myeong [16] this work emphasizes on using machine learning (ML) methods (support vector machine (SVM), XGBoost, and artificial neural networks (ANN)) to develop industry standards for cloud computing security (CCS). The objectives of machine learning study are achieved by selecting these eleven crucial features. This study finds limitations in cloud cyber security's (CCS) application of machine learning (ML) approaches. Moreover, the goal of this research is to create an achievable strategy for anticipating machine learning use in an industrial cloud context with respect to privacy and trust concerns. Through utilizing accuracy, R.O.C., F1 scores, curves, confusion matrices (CM), and validation matrices of recall, and precision values, the efficacy of the utilized models is evaluated. M. Roshanaei, M. R. Khan, and N. N. Sylvester [17] this study highlights the new threats produced by these technologies and investigates the essential role that ML (machine learning) and AI (artificial intelligence) play in improving cybersecurity (CS) defenses against more complex cyberattacks (CA). The dual-edged nature of AI (artificial intelligent) and ML (machine learning) in CS (cybersecurity) is being explored by a comprehensive examination covering historical trends, and predictive modeling. The study addresses significant issues comprise data protection (DP), continuous training of AI (artificial intelligent) models, risks of manipulation, and ethical dilemmas. The work introduces a comprehensive approach that utilizes innovative technology combined with strict ethical principles and robust CS (cybersecurity) measures. This strategy facilitates various stakeholders to work together to generate policies that ensure the ethical and efficient application of AI in cybersecurity, with the aim of improving scheme integrity and privacy without sacrificing security. O. F. Hassan et al. [18] create a survey research, with 890 cloud experts along with knowledge of CC (cloud computing) and CS (cybersecurity) providing data for the work. The authors utilized a machine learning (ML) methodology, applied a random forest (RF) classifier, an ensemble, and a decision tree (DT) model. To achievement the aim of the work, ten distinct attribute were chosen from the data rely on the importance of the random forest (RF) attribute. The goal of the research is to provide organizations with the necessary tools to utilize random forest (RF) predictions to prevent cybercrime in relation to cloud services in the united states (US). U. A. Butt et al [19] analysis of CCS (cloud computing security) concerns, challenge, and solutions in this research paper employing one or more machine learning (ML) techniques. Moreover, the work examines several machine learning (ML) techniques, including SL (supervised learning), UL (unsupervised learning), SSL (semi-supervised learning), and RL (reinforcement learning), to address CS (cloud security) concerns. After that, we evaluate the performance of each technology through comparing its drawbacks and benefits. Moreover, we list directions for future studies to secure cloud computing (SCC) models. A. Ahmed, et al [20] this paper presents a trust-based routing protocol (TrustML-RP) with machine learning (ML)-enablement that can identify attacking nodes behind packet suppression attacks and distributed denial of service (DDoS) attacks. In order to establish a trust factor among participating nodes, the proposed TrustML-RP scheme first adopts the distributed trust model. After that, it utilizes an effective combination of machine learning (ML) techniques, e.g. artificial neural networks (ANN) and support vector machines (SVM), to identify attacker nodes and obtain the best and most secure route. To describe the effectiveness of the suggested scheme on a network of a reasonable size with mixed nodes, a comprehensive performance evaluation is conducted. The results demonstrate how successful the proposed plan is improving network security and generating a trustworthy network environment. According to the study's results, cybersecurity (CS) experts can generate more successful cybersecurity (CS) schemes through combining machine learning (ML) approaches with a trust-based model to enhance traditional cybersecurity (CS) practices. Mr. B. Srinivas et al. [21] presents a comprehensive analysis of machine learning (ML) algorithms utilized in the area of cybersecurity (CS), comprise RL (reinforcement learning), UL (unsupervised learning), and SL (supervised learning). utilizing regression and classification techniques, supervised learning (SL) techniques such as decision trees (DT), support vector machines (SVM), and neural networks (NN) are analysed to determine how well they identify known risks. It is examined whether unsupervised learning (UL) techniques, like as clustering and anomaly detection (ND) algorithms, can identify unknown and zero-day threats through identifying deviations from typical behavioral patterns. Since reinforcement learning involves learning the best defense techniques by interacting with the environment, its potential to enhance proactive security measures is being investigated. The paper investigates the real-world applications of these techniques, such as network traffic analysis (NTA), malware, phishing (MP), and intrusion detection systems (IDS). To illustrate the

DOI: 10.31695/IJASRE.2024.8.10

observable benefits and challenges associated with deploying machine learning (ML)-driven cybersecurity (CS) solutions, the work examines case studies and practical applications. M. Marwan, A. Kartit, and H. Ouahmane [22] this paper introduces a completely new approach to secure data processing in cloud environments based on machine learning techniques. To identify image pixels more effectively, we typically employ fuzzy C-means clustering (FCM) and support vector machines (SVM). To further lower the danger of possible medical information disclosure, we integrate an additional layer, the CloudSec module, into the standard two-layered structure. To test the proposed method, we conducted two sets of experiments. The simulation results show that Support Vector Machines (SVM) are a useful idea for data protection and image segmentation (IS) at the same time. Ultimately, we have obtained some promising results that provide new perspectives for the development of cloud services in healthcare. D. Praveena and P. Rangarajan [23] this paper introduces a novel cloud service indicates hybrid cloud service (HCS), which combines public and private cloud computing. These days, cloud security is a difficult issue, especially for hybrid clouds because of their combination of the two. In this research, we suggest a novel machine learning application that secures hybrid cloud networks while storing, retrieving, and allowing access to data. This approach combines the recently proposed dynamic access control mechanism, the newly suggested deduplication processing technique, and the already-existing Enhanced C4.5. Additionally, we present a novel deduplication processing approach that ensures secure storage and retrieval without redundancy or duplication. The proposed security framework also uses the dynamic access control mechanism of the recently announced dynamic spatial role-based on access control (AC) algorithm. Implement the proposed security architecture and evaluate the security level of the hybrid cloud while storing, accessing and retrieving data from the cloud dataset. T. Salman et al. [24] in this paper, as is common in current research work, we examine both the identification and classification of anomalies. We have developed and tested learning models for both detection and classification of various attacks using a widely used publically accessible dataset. Specifically, we have utilized two supervised machine learning (ML) methods: RF (random forest) and LR (linear regression). We show how similarities between attacks can lead to less accurate classification even in cases where detection is fault-free. Our findings show a detection accuracy of over (99%) and a categorization accuracy of (93.6%), while many attacks cannot be classified. Furthermore, we contend that the same machine learning (ML) methods can be used to apply similar categorization to multi-cloud systems. M. Rabbani et al. [25] this paper proposes a new strategy to improve the ability of cloud service providers (CSP) to simulate user behavior. For the aim of detection and recognition, we utilized a particle swarm optimization-depend on probabilistic neural network (PSO-PNN). Using a multi-layer neural network (MLNN), we first classified and identified the dangerous behaviors in the user behavior data after meaningfully transforming it into an understandable format. We used the UNSW-NB15 dataset to characterize various forms of malicious behavior displayed through users in order to validate the suggested approach. The proposed approach has potential application in security monitoring and malicious behavior identification, as evaluated through experimental data. G. Nicholas and D. Karan [26] the study examines the effectiveness of both supervised learning (SL) and unsupervised learning (UL) models, emphasizing how flexible they are in response to changing threat environments. The study also explores how machine learning (ML) can improve real-time incident response times and serve as a continuous training tool to adapt to evolving security threats. By an analysis of the mutually advantageous interactions among cloud security (CS) and machine learning (ML), this article objective to provide a complete review of state-of-the-art techniques and presents insights into the evolving field of secure cloud computing (SCC). M. N. R. Khan et al. [27] in this review, the literature on machine learning and its applications in online-based data security frameworks for malware detection (MD), prevention, and use—such as email filtering—is examined in this article. Based on the importance and amount of citations, each strategy has been described and summarized. Many well-known databases are frequently cited because of the significance of datasets in machine learning (ML) techniques. Additionally, some usage guidelines for specific algorithms are provided. Four machine learning (ML) algorithms were utilized to evaluate the MODBUS data that came from a gas pipeline. Machine Learning (ML) methods were used to classify a number of attacks, and the final evaluation of each technique was based on its efficiency. N. Tabassum, et al. [28] this research article focuses on the security, dependability, and potential performance of cloud services. In order to measure the security, privacy, and trust aspects of cloud security, the machine learning (ML) algorithm neuro-fuzzy has been employed in this work. The results show that the main purpose of the ANFIS-dependent parameters is to identify anomalies in cloud security (CS). The characteristics output typically produces superior outcomes and ensures computing power and data consistency. M. Alsharif and D. B. Rawat [29] this paper proposes a cloud-based service architecture to manage machine learning models optimally adapted to various operational

DOI: 10.31695/IJASRE.2024.8.10

configurations of IoT devices for security. This service could help an IoT device reduce the maintenance burden of an intrusion detection system by moving heavy tasks, comprise feature selection (FS), model creation, training, and validation, to the cloud. The internet of things (IoT) device would then receive the security model back from the cloud as a service.

5. COMPARATIVE ANALYSIS FOR MACHINE LEARNING (ML) IN CYBER SECURITY (CS)

Table 1 shows a summary of all the previous work described above on machine learning (ML) models to enhance cybersecurity (CS).

Table 1.1 Pervious work summary

Year	Study	Focus	Propose of the review	Future work
2023	Z. Abbas and S. Myeong [16]	Enhancing cloud computing security (CCS) with machine learning (ML) techniques	-Aims to provide an effective strategy for prediction using machine learning (ML) in an industrial cloud environment (ICE) with respect to privacy and trust difficulties. - It highlights the significance of implementing continuous development and research in order to produce more developed and effective security solutions for cloud computing.	- Using novel characteristics that can improve the models' efficacy. To evaluate their performance with the chosen models, other machine learning (ML) models like RF (Random Forest), DT (Decision Trees), and NB (Naive Bayes) can be employed. - The dataset may comprise many instances and different characteristics.
2024	M. Roshanaei, M. R. Khan, and N. N. Sylvester [17]	Artificial intelligent (AI) and machine learning (ML) in improving cybersecurity	Highlights a comprehensive approach that leverages the use of advanced technology combined with strict ethical guidelines and effective cybersecurity procedures.	Requires being focused on creating reliable systems that are able to recognize and prevent these kinds of manipulative attempts.
2024	O. F. Hassan et al. [18]	Enhancing cybersecurity (CS) through cloud computing (CC)	Providing organizations with the techniques to use Random Forest (RF) predictions to prevent cybercrime related to cloud computing services (CS) in the United States (US).	-Further research in this area should consider collecting large amounts of data and implementing different machine learning models to investigate how cloud computing (CC) improves cybersecurity (CS) in the United States (US).
2020	U. A. Butt et al [19]	Machine learning (ML) methods in Cloud Computing Security (CCS)	Present a review of the risks, problems, and solutions related to cloud computing (CC) security which used one or more machine learning (ML) methods.	Presented a number of research directions that require further study in the future
2023	A. Ahmed, et al [20]	Improving cybersecurity (CS) by the utilize of machine learning (ML) techniques	Proposing a trust-based routing protocol (TrustML-RP) with machine learning (ML) support that identifies attacker nodes behind distributed denial of service (DDoS) and packet suppression attacks (PSA).	

DOI: 10.31695/IJASRE.2024.8.10

2024	Mr. B. Srinivas et al. [21]	Machine Learning (ML) Methodologies in Cybersecurity (CS)	Examines machine learning techniques used in cybersecurity in detail, including (RL(reinforcement learning), UL (unsupervised learning), and SL (supervised learning)).	
2018	M. Marwan, A. Kartit, and H. Ouahmane [22]	Machine Learning (ML) techniques for enhancing secure data in cloud computing (CC)	Proposing an innovative strategy to secure data processing in cloud environments based on machine learning (ML) techniques. To identify image pixels more effectively, we typically employ two techniques (fuzzy C-means clustering (FCM)and support vector machines (SVM)).	Focus on performing increasingly complex image processing operations.
2020	D. Praveena and P. Rangarajan [23]	Machine learning (ML) application in hybrid cloud networks (HCN)	Suggest a novel machine learning (ML) application that will protect hybrid cloud networks while enabling data storage, retrieval, and access.	Using effective encryption technology to provide secure storage.
2017	T. Salman et al. [24]	Supervised machine learning (SML) techniques for Anomaly Detection(AD) in multi-cloud Environments (MCE).	Employing the supervised machine learning techniques of linear regression (LR) and random forest (RF) Exploring methods for anomaly detection and classification.	
2020	M. Rabbani et al. [25]	A hybrid machine learning (ML) approach in cloud computing (CC)	Proposed approach aims to improve the capacity of cloud service providers (CSPs) to accurately model customer behaviors.	Deep learning techniques and new anomaly observations in zero-day attacks and vulnerabilities aim to improve the proposed approach.
2024	G. Nicholas and D. Karan [26]	Supervised learning (SL) and unsupervised learning (UL) models for secure cloud computing (SCC)	Highlighting its ability to adapt to changing threat environments	Presented a number of research directions that require further study in the future
2022	M. N. R. Khan et al. [27]	Machine Learning (ML) algorithms for attack in cybersecurity (CS)	Provides an analysis of the research on machine learning (ML) and its application to online data security frameworks for email filtering (EF) and other malware prevention (MP), labeling, and utilization.	required to evaluate the results of algorithms because the dataset distorts the efficiency of the algorithms. Due its ideal real-time performance, random forest (RF) might be more suitable as the primary IDS algorithm in the current scenario.
2022	N. Tabassum, et al. [28]	Machine learning (ML) algorithm for cloud security (SS)	-Suggested using a machine learning (ML) technique known as Neuro-Fuzzy (NF) to measure security parameters,	

DOI: 10.31695/IJASRE.2024.8.10

			issues of privacy, and trust difficulties related to cloud security.	
2021	M. Alsharif and D. B. Rawat [29]	Cloud-As-a-Service IoT Security with Machine Learning (ML) Models	Propose the most suitable machine learning (ML) models for different IoT device operation scenarios for security through cloud-based service structure.	-Validation of the Cloud MaaS concept on real-world embedded systems and cloud service algorithms for various types of Internet of Things devices

6. CONCLUSION

The utilize of machine learning (ML) models to enhance cybersecurity (CS) has been a growing trend in the past few years. The aim of the article is to propose a comprehensive study of all techniques to predict the utilizing of machine learning (ML) models in the cloud computing (CC) environment. The article focuses on recent years and provides the most recent methodologies machine learning (ML) in a wide range of cybersecurity problems across many different types of application areas including cyberbullying detection (CBD), zero-day attack detection (ZDAD), spam filtering (SF), fraud detection (FD) and anomaly detection (AD), malware analysis (MA) and detection, intrusion detection (ID), threat analysis (TA), and IoT attacks. In addition to comparing the study to previous works. The article demonstrates the findings that enhance cybersecurity using machine learning (ML) models for play critical roles in organizations to make informed and more accurate decisions and can be suitable for utilization as an accurate prediction model.

REFERENCES

[1] A. B. Nassif, et al., "Machine learning for cloud security: a systematic review," IEEE Access, vol. 9, pp. 20717-20735, 2021.
[2] A. Aljumah and T. A. Ahanger, "Cyber security threats, challenges and defence mechanisms in cloud computing," IET communications, vol. 14, no. 7, pp. 1185-1191, 2020.
[3] S. Achar, "Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape," International Journal of Computer and Systems Engineering, vol. 16, no. 9, pp. 379-384, 2022.
[4] Jupalle, et al., "Automation of human behaviors and its prediction using machine learning", Microsyst. Technol. 2022, 28, 1879–1887.
[5] T. L. Duc, R. G. Leiva, P. Casari, and P.-O. Östberg, "Machine learning methods for reliable resource provisioning in edge-cloud computing: A survey," ACM Computing Surveys (CSUR), vol. 52, no. 5, pp. 1-39, 2019.
[6] K. Li, et al., "Assessment of Machine Learning Algorithms in Cloud Computing Frameworks", Proceedings of the 2013 IEEE Systems and Information Engineering Design Symposium, University of Virginia, Charlottesville, VA, USA, April 26, 2013.
[7] M. Callara and P. Wira, "User behavior analysis with machine learning techniques in cloud computing architectures," in 2018 International Conference on Applied Smart Systems (ICASS), 2018, pp. 1-6: IEEE.
[8] N. A. Azeez, B. B. Salaudeen, S. Misra, R. Damaševičius, and R. Maskeliūnas, "Identifying phishing attacks in communication networks using URL consistency features," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 2, pp. 200-213, 2020.
[9] A. A. Nureni and I. C. Chinyere, "Machine Learning in Cyber Security Operations," *University of Ibadan Journal of Science and Logics in ICT Research*, vol. 11, no. 2, pp. 57-70, 2024.
[10] F. Liu and J. Wang, "RETRACTED ARTICLE: A User-Centric Machine Learning for Learning Support System with Adequate Cyber Security," *Wireless Personal Communications*, vol. 127, no. Suppl 1, pp. 19-19, 2022.
[11] Tanium, "Machine Learning in Cybersecurity: A Primer for Beginners," https://www.tanium.com/blog/machine-learning-in-cybersecurity/
[12] P. Walpita, "Types of Machine Learning,"
https://www.linkedin.com/pulse/types-machine-learning-priyal-walpita

DOI: 10.31695/IJASRE.2024.8.10

[13] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255-260, 2015.
[14] E. Proko, A. Hyso, and D. Gjylapi, "Machine Learning Algorithms in Cyber Security," in *RTA-CSIT*, 2018, pp. 203-207.
[15] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects," *Annals of Data Science*, vol. 10, no. 6, pp. 1473-1498, 2023.
[16] Z. Abbas and S. Myeong, "Enhancing industrial cyber security, focusing on formulating a practical strategy for making predictions through machine learning tools in cloud computing environment," *Electronics*, vol. 12, no. 12, p. 2650, 2023.
[17] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions," *Journal of Information Security*, vol. 15, no. 3, pp. 320-339, 2024.
[18] O. F. Hassan *et al.*, "Enhancing Cybersecurity through Cloud Computing Solutions in the United States," *Intelligent Information Management*, vol. 16, no. 4, pp. 176-193, 2024.
[19] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electronics*, vol. 9, no. 9, p. 1379, 2020.
[20] A. Ahmed *et al.*, "Enhancing Cybersecurity with Trust-Based Machine Learning: A Defense against DDoS and Packet Suppression Attacks," *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, vol. 23, pp. 262-268, 2023.
[21] Mr. B. Srinivas *et al.*," Enhancing Cybersecurity with Machine Learning: Algorithms and Approaches", International Journal of Intelligent Systems and Applications in Engineering, ISSN:2147-67992, vol. 12, no. 22s , pp. 210–220, 2024.
[22] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388-397, 2018.
[23] D. Praveena and P. Rangarajan, "A machine learning application for reducing the security risks in hybrid cloud networks," *Multimedia Tools and Applications*, vol. 79, no. 7, pp. 5161-5173, 2020.
[24] T. Salman *et al.*, "Machine learning for anomaly detection and categorization in multi-cloud environments," in *2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud)*, 2017, pp. 97-103: IEEE.
[25] M. Rabbani *et al.*, "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing," *Journal of Network and Computer Applications*, vol. 151, p. 102507, 2020.
[26] G. Nicholas and D. Karan, "Machine Learning Algorithms for Cloud Computing Security", Department of Computer Engineering, University of Harvard, 2024.
[27] M. N. R. Khan *et al.*, "Machine learning approaches in cybersecurity," in *Data Intelligence and Cognitive Informatics: Proceedings of ICDICI 2021*: Springer, 2022, pp. 345-357.
[28] N. Tabassum, *et al.*, "Qos based cloud security evaluation using neuro fuzzy model," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1127-1140, 2022.
[29] M. Alsharif and D. B. Rawat, "Study of machine learning for cloud assisted iot security as a service," *Sensors*, vol. 21, no. 4, p. 1034, 2021.

DOI: 10.31695/IJASRE.2024.8.10