Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cloud Security: A Review Based on Machine Learning Techniques

Manpreet Kaur*
**PG Department of Computer Science, Mata Gujri College, Fatehgarh Sahib, Email: manpreetkaur.mgc@gmail.com*

ARTICLE INFO

Received: 15 Sep 2022

Accepted: 22 Oct 2022

ABSTRACT

Introduction: The rapid adoption of cloud computing has introduced scalable, on-demand services; however, it has also exposed critical security vulnerabilities across different layers of cloud.

Objectives: This review aims to comprehensively investigate the major security threats in cloud environments, assess Machine Learning (ML) techniques employed to address these threats, and identify the open research challenges that hinder robust cloud security.

Methods: A total of 57 articles were systematically analysed using a defined search string across major digital libraries like IEEE, Science Direct and so on while following few includion exclusion criteria for selecting papers related to objective.

Results: The findings reveal that Distributed Denial-of-Service (DDoS) attacks and network intrusions are the most frequently addressed threats, with ML models such as SVM, KNN, RF, and hybrid ensemble frameworks being widely adopted for detection and mitigation. Despite these advancements, challenges such as computational overhead during training, limited multi-attack coverage, outdated benchmark datasets, and lack of generalizability to real-world scenarios persist.

Conclusions: This review highlights the need for scalable, real-time, and intelligent security frameworks using ML/DL to effectively safeguard cloud infrastructures against evolving cyber threats.

Keywords: Cloud Security, ML in Cloud, Cyberattack detection etc.

INTRODUCTION

In the past, IT firms obtained the necessary services by using on-premise technology, or conventional computing methods. Even though these techniques are safe, IT firms still have to deal with a lot of issues including backups, capacity, and cost [1]. Over time, as digital communication evolved and internet usage became deeply integrated into daily operations across sectors—such as healthcare, defense, electronics, private firms, education, and industry—the reliance on conventional systems began to fade. The internet has now become a backbone for global connectivity, and its absence would almost paralyze modern life. As a result, cloud computing has gained a lot of attention lately because of the growing need for safer and more effective means of communication and network storage of large data [2]. The way businesses obtain digital services has changed as a result of cloud computing. Organizations can increasingly depend on third parties who offer a variety of services via the internet in place of setting up and running their own network. These suppliers supply a wide range of services, including networking tools, software programs, data storage, and processing power [3]. In simple terms, cloud computing frees users from having to handle the physical components or systems and permits them to get hold of whatever resources they require, like processing power or storage space, wherever they may require. This on-demand model is a very flexible and effective solution because it guarantees that consumers can swiftly scale their consumption up or down based on their unique requirements.

The idea behind the centre is to allow systems to customize tasks as needed without any human intervention. To ensure such services, CC comprises of three services models named as SaaS (Software as a Service) which deals with user based request to software's like email, IaaS (infrastructure as a Service) for providing hardware resources to user like CPU, memory and storage and lastly PaaS (Platform as a Service) which allows designing, execution and administrating applications respectively. Furthermore, these models can be deployed under three categories of Public, private and hybrid clouds [4]. Public, private, and hybrid clouds are among the deployment options that cloud computing enables [4]. Private servers are handled by a single company that offers greater control and security than public servers, which

are run by third parties and are available to everyone. Hybrid clouds offer a well-rounded alternative for a range of requirements by combining aspects of both. Usually, hybrid clouds are used by enterprises for exploiting the benefits of private as well as public clouds. Some of the major company's including AWS and Microsoft Azure own around 32% and 20% of the cloud market share while google cloud platform and Alibaba cloud own around 7.7% and 4.6% market share of cloud.

The growing popularity of cloud computing has raised significant worries about data safety, especially with regard to protecting user information's confidentiality, integrity, and availability (CIA). From publicly available files to highly sensitive and private data, cloud-based services are built for handling and safeguard information of all sensitivity levels. They must simultaneously provide users with smooth, 24/7 access to computer resources. Nonetheless, the cloud's constant operation and extensive data storage capacity make it a desirable target for cybercriminals. Attackers are always looking for ways to breach one or more CIA triad components, which might make people less trusting of the system [5]. Moreover, the likelihood of introducing fresh viruses or undetectable viruses, like zero-day malware, is greatly raised by the enormous volumes of data that are kept or transferred amongst the cloud and users [6]. As a result, the conventional methods and procedures that are employed to safeguard the cloud infrastructure, identify anomalies and maintain confidentiality are ineffective. Therefore, more effective methods ought to be employed to improve security in the cloud [7]. Over the years, Machine learning (ML) has gained much attention for greatly improving cloud computing safety.

ML has emerged as a powerful tool in the fight against both traditional cyberattacks and more sophisticated threats like zero-day exploits. Fundamentally, machine learning operates on a range of methods that can analyze data, uncover undetected trends, and use that knowledge to make predictions. ML improves systems' capacity to predict and react to possible vulnerabilities more precisely by fusing aspects of statistical computing and computational science. In general, machine learning methods can be divided into three primary groups: supervised learning, which involves training a system on labelled data; unsupervised learning, that identifies trends in unlabelled data; and semi-supervised learning, which combines the two methods to enhance performance when labelled data is scarce [8].

In contrast to more conventional methods like firewalls, intrusion detection systems (IDSs), and antivirus software, machine learning has proven a very effective way for safeguarding cloud servers given that it can assess big data flows, identify risks, weaknesses, and violations in the cloud environment—particularly unknown attacks and utilize historical data to understand patterns[9]. Additionally, by safeguarding the equipment's dependability, upholding the system's quality, and extending its lifespan, machine learning approaches are employed in cloud computing to make resources available. These tactics guarantee preventing data loss and service interruptions.

The major objective of this study is to review various ML techniques and methods utilized in current cloud systems for detecting or protecting it from attacks and vulnerabilities.

REVIEW METHODOLOGY

This review's primary goal is to examine the urgent security concerns that still jeopardize the reliability of cloud computing platforms. Conventional safety measures are becoming less and less effective as a result of the variety and breadth of threats that have increased dramatically with the acceleration of cloud usage across companies. This paper delves deeper into how Machine Learning (ML) approaches are emerging as viable remedies for these changing threats. These clever techniques can more accurately detect known and unknown assaults, analyze massive amounts of cloud traffic, and spot unusual activity.

- *Search Strategy*

A fundamental step in conducting an effective review is the precise definition of the research scope, followed by the identification and selection of the most relevant scholarly literature aligned with the topic. To support this process, several reputable digital libraries were utilized as primary sources for academic publications including;

- ScienceDirect
- IEEE Xplore
- ACM Digital Library
- Google Scholar

An extensive literature search was conducted, covering both foundational and recent works related to cloud computing security. The selection focused on research discussing cloud-specific threats, vulnerabilities, security challenges, and the application of ML techniques for mitigating such issues. The following search string was used across databases to ensure

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

comprehensive coverage: (cloud computing) AND security AND (attack OR issues OR threats OR challenges) AND (machine learning OR ML). This systematic approach ensured that only the most pertinent and high-impact studies were considered for analysis in this review.

- *Study Selection*

An initial pool of 230 research articles was retrieved using the defined search criteria. To ensure the quality and relevance of the review, a multi-stage filtering process was applied by the authors. This process involved evaluating the content against predefined inclusion parameters, resulting in a refined selection of studies as outlined in Table 1.

Table 1: Inclusion and Exclusion criteria for Review

S. no	Inclusion Conditions	Exclusion Conditions
1	ML technique for cloud security	Papers evaluation is not cloud based.
2	Using hybrid ML or other models for cloud systems	Repeated papers
3	Journal and conference papers only	Non-published papers
4	Papers with specific Cloud Topic	Papers not related to cloud security or ML
5	Referenced publications	

After selecting papers based on this criteria, we are left with 57 papers only which are referenced in this paper.

- *Research Questions*

The selected case studies were thoroughly analyzed to address the core research questions outlined in Table 2. The purpose of these study topics is to identify the crucial part machine learning plays in protecting cloud systems from a variety of security threats. The answers to these questions are intended to demonstrate how machine learning approaches help reduce risks and improve cloud safety on a variety of aspects.

Table 2: Research Questions Framed

S.no	Research question
RQ1	Identify which security issues make CC vulnerable to attacks?
RQ2	What are the major threats faced in CC environments over time?
RQ3	Which ML techniques or approaches have been put forward for enhancing security in cloud systems

THREATS IN CLOUD SYSTEMS

Any vulnerability within a CC environment can compromise one or more of the core pillars of information security commonly referred to as the CIA triad [10]. The following section provides a concise overview of the major threats that pose risks to these fundamental security principles in cloud systems.

There are three types of cloud computing vulnerabilities that jeopardize secrecy [11]: primarily external attempts resulting in damage or illegal access to cloud-based applications or disclose stored information by unauthorized parties using distant computers or software for their own malevolent ends. The next category is insider attacks, whereby a legitimate platform is used for malevolent objectives by an insiders, who may be a staff member in the cloud, exposing cloud information or harming or gaining unwanted access to cloud apps [12]. Lastly, privacy risks that arise from a lack of safety devices, incorrectly configured security tools, user error, secured access breakdowns, etc.

The Problems regarding cloud computing which jeopardize confidentiality of data include dangers associated with content separation, problems with access management, and authorization, which protects data from alteration. Initially because of the modifications that occur in the computing environment for the resources linked to the users, the dangers associated with content separation impact data quality. These could be the results of poorly designed virtual machines and clumsy client-side hypervisors [13]. Secondly, failure to adhere to the strategy that outlines who is authorized to use cloud services or to apply security measures like biometrics, passwords, or usernames can result in problems with authenticate and access management [14]. Lastly, protecting the data from purposeful or inadvertent alteration. Since customer information is saved on the clouds, the cloud providers bears the responsibility for maintaining data authenticity.

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Availability in cloud computing can be compromised by several types of threats, each affecting users' ability to reliably access cloud-based services and resources. One major concern is service inaccessibility, often caused by external threats such as DoS attacks. These can prevent users from reaching essential components like data transfer channels, DNS servers, software applications, or other hosted assets. Another key factor involves physical or operational disruptions, which may originate from the IT infrastructure failures of cloud service providers, the customers' internal IT systems, or connectivity issues introduced by network providers such as wide area network (WAN) operators. Lastly, ineffective backup and recovery strategies also pose a risk to availability. If reliable data recovery mechanisms are not in place, system outages or data losses can result in prolonged service downtime and significant operational setbacks [15].

MAJOR ATTACKS ON CLOUD ENVIRONMENTS

While analysing major security concerns in cloud computing (CC), I reviewed a vast body of research and observed that several significant attacks have targeted different layers of the cloud architecture over the years. Among the vast attacks, DDoS (Distributed Denial-of-Service) attack stand out as most frequent and damaging one. These kind of attacks have the potential to overload cloud servers with congestion, disrupting normal operations. Over the years, ML techniques were deployed for differentiating between fraudulent and legitimate messages to identify and counteract such breaches [16]. Additionally, authors in [17] utilized advanced techniques like selective cloud egress filter (SCEF) for detecting and blocking virtual machines (VMs) involved in DDoS attacks to stop such assaults. The difficulties in protecting against DDoS attacks in cloud environments are highlighted by the rapid rise in internet traffic and the unpredictable nature of attacks [18]. Another serious risk is posed by VM escape attacks, which let hostile VMs bypass isolation borders for obtaining access to other VMs or the host computer system without authorization. These flaws provide a serious security risk to cloud environments, highlighting the necessity of strong security measures and ongoing observation to stop unwanted access.

Cloud computing's Platform as a Service (PaaS) layer poses unique security risks that could jeopardize privacy and authenticity. The use of insecure APIs, which are the main means for interacting between apps, represents one of the main issues at this tier. Such APIs are susceptible to a variety of dangers because they have not been properly developed, missing input/output validation, verification, and authorization. These flaws could be used by attackers to alter services, get around access restrictions, or access private cloud data without authorization. For instance, unapproved data exposure or manipulation may arise from misconfigured authentication systems or from the lack of strong data validation procedures [19]. The man-in-the-middle (MITM) attack is yet serious danger that puts PaaS environments at serious risk. In some situations, hackers steal data while it's in transit, possibly changing or acquiring private data before it gets to its recipient. According to certain studies, MITM attacks affect information security and secrecy by taking advantage of flaws in the transmission routes [20]. Various security solutions can be used to lessen these problems. The use of encryption and strong authentication processes can be used to secure APIs and preserve confidential information and authenticity. Furthermore, periodic inspection and monitoring of APIs can assist in locating and fixing possible flaws before attack. Moreover, by using effective encryption protocols like SSL/TLS sensitive information can be encrypted during transmission by making it more difficult for attackers to capture interactions. Another preventive measure is using intrusion detection and prevention systems (IDPS) to keep an eye on communication for strange patterns that could point to an MITM attack.

The application layer, or SaaS, is especially susceptible to a number of security risks, such as session hijacking and SQL injection. In SQL injection attack, hackers can modify the database's backend and retrieve or change sensitive data by inserting malicious code into database queries. On the other side, session hijacking is intercepting and using active user sessions without authorization in order to obtain restricted information or features. Experts have put out a number of detection and mitigation strategies to cope with these hazards, many of which use ML to improve precision and flexibility. Based on its structure and behaviour, studies have used models like CNN-BiLSTM architectures, DT, SVMs, and NN to categorize SQL queries as safe or dangerous [21]. Notably, a dedicated CNN-based approach was introduced in [22] to detect SQL injection payloads from network traffic data. This method outperformed traditional rule-based systems by offering greater resistance to obfuscation techniques and delivering higher detection accuracy.

In addition to these frequently occurring attacks, there are some other attacks as well including APTs (Advanced Persistent Threats), Spectre and Meltdown. APTs which is also known as Zero Day or Silent Attack obtains unauthorized prolonged access to cloud server for continuously stealing data while hopping from one data centre to another. This attack is highly challenging for typical IDS to detect since it may adjust to the defensive measures [23]. Furthermore, recent versions of processors contain a design flaw which attackers take advantage of to get possession of storage and

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

reveal encrypted information using Spectre and Meltdown attacks. Since each of these attacks have their roots in the framework of the kernel and reveal details, the segregation of apps and OSs is thus destroyed [24].

ANALYSIS AND CRITICAL REVIEW OF ML BASED CLOUD SECURITY APPROACHES

In this particular section, a detailed analysis was conducted to understand the impact of ML approaches on security of CC systems. This analysis's main goal is to draw attention to how important cloud environment security is and how urgent it is to protect them from a variety of attacks and loopholes. This assessment looks at the many machine learning (ML) techniques used to identify, stop, and minimise attacks in the cloud. Furthermore, the study answers the primary research questions (RQ1–RQ3).

Table 3: Analysis of various techniques for improving Cloud Security.

Reference	Problem or Attack Type	Proposed Technique	Results
[25]	Problems in Zero-Trust VPC Systems	Implemented a hybrid system combining RL-Q Matrix, VGAN, multi-server queuing, and authentic VPC within the MLSCS framework during scheduling process.	Around 5%–8% improvement over to RLDH, CSOS, and FSDS
[26]	Unauthorized Data Access	Proposed SVM and FCM based model for preventing unauthorized access to data within CloudSec-enhanced architecture.	Improved results over traditional 2 layer models.
[27]	DDoS	Developed SAE-ELM-CA with optimized crossover and neuron selection	Attained highest accuracy of 99.99% on CICIDS database and lowest Accuracy of 86.80% on NSL-KDD.
[28]	Addressing security in VB5G cloud networks	Proposed ML based technique integrating differential privacy and Paillier Homomorphic Encryption, along with IDS to safely transfer data over 5G networks	Outperformed traditional IDSs in terms of accuracy, CPU usage, response speed, and secure communication
[29]	DDoS	Proposed ANN inspired security system using V-ELM for detecting DDoS attacks.	Highest Acc=99.18% on NSL-KDD and 92.11% on ISCX.
[30]	Malicious mining code detection in Cloud	Applied ML based Bagging and Boosting-based ensemble model that analyses mining file strings for feature extraction	AUC= 99.2% F1= 98% SD=0.0009
[31]	Unusual User Behaviour	Introduced a hybrid detection model using optimization based system suing PSO-PNN.	It can only detect unusual user behaviour
[32]	Intrusions in mobile cloud with diverse client networks	Proposed IDS based on ML that could detect MITM and DDoS Attacks.	Adaptable to client diversity for detecting MITM and DDoS
[33]	APT	Proposed auto-encoder-based DL approach with Softmax regression for traffic classification	ACC= 98.32% and better than ML models like SVM.
[34]	Ransomware and RAT detection in VMs	Proposed a Random Forest-based framework using meta-feature extraction from Linux volatile memory dumps	TPR = 1, FPR = 0.052, AUC = 0.966, and F-measure = 0.976
[35]	Malware Identification	Introduced a semi-supervised transfer learning (SSTL) model combining byte-level RNN classification and ASM prediction	ACC= 96.9%.

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[36]	NIDS	Utilized SVM as a base classifier for detecting network intrusions and evaluated multiple ensemble approaches	ACC=98.7%
[37]	DDoS attack filtration	Proposed a statistical-based method aimed at identifying and filtering DDoS and TCP-based attacks	Low FAR ACC=94%
[38]	Adaptive DDoS	Designed a self-learning detection system leveraging NetFlow protocol for traffic monitoring and periodic model retraining	ACC= 95% F1=94% and minimal FPR in distinguishing normal and malicious users
[39]	Intrusions in multi-cloud environments	Proposed ML based intrusion identification system based on historical data and also used de-noising Auto-encoder.	ACC=95%
[40]	DDoS attack classification using ML firewalls	Applied multiple machine learning models—RF, SVM, and NB to identify and classify malicious traffic in cloud firewalls	RF ACC= 98% SVM ACC=99% NB ACC= 97%
[41]	Ensuring trust and reducing job scheduling costs	Introduced the MMA (Matching and Multi-Round Allocation) scheduling algorithm aimed at minimizing job make- span and overall cost while preserving system reliability and security	Lowered processing time and improved resource utilization.
[42]	Minimizing computational overhead	Proposed a multi-party learning framework based on Backpropagation Neural Network (BPNN), allowing data encryption at the user level before cloud-based training	Effective for protecting sensitive data.

In addition to above mention techniques there are plenty of other ML techniques proposed by researchers for detecting cyberattacks. He et al., in [43] introduced a detection framework aimed at identifying DoS attacks at their origin within cloud environments. Basically, they examined the statistical characteristics of various common DoS variants, including flooding, spoofing, and brute-force attacks, which are among the most frequently encountered types of DDoS threats. Similarly, Kumar et al., in [44] developed an IDS called Eucalyptus, specifically designed to safeguard VMs in cloud environments against DoS attacks. This platform is capable of identifying malicious activity originating from both internal and external sources across the internet.

Nevertheless, authors in [45] proposed NIDS for cloud systems specifically for identifying and blocking DoS attacks and other forms of malicious behaviour at the network layer. They achieved this milestone by continuously monitoring traffic to detect anomalies while ensuring that the overall system performance and quality of service are not compromised. In contrast, Khorshed et al. in [46] introduced a Proactive Attack Detection framework to identify cyberattacks either at the onset or during execution and notifies users if there was any attempt by the cloud provider to suppress attack-related information. Through tests, they identified SVM as the most effective technique for their detection mechanism.

Researchers in [47], proposed an approach aimed at enhancing cloud system security and performance. They observed that persistent uncertainty around data confidentiality, particularly when third-party entities were responsible for storing and processing sensitive information still exists. To mitigate this issue, the authors employed ANN over scrambled data to detect and manage potential threats. In a related effort, the author's in [48] introduced threat classification framework that leverages ML techniques for identifying and addressing security vulnerabilities in cloud. Additionally, they also proposed a cloud risk categorization model, utilizing ML techniques to accurately differentiate between various threat levels and respond accordingly.

Selamat et al. [49] investigated the application of ML algorithms in addressing malware-related threats within cloud computing environments. Later they introduced a barrier-based framework that evaluates three different ML models, ultimately selecting those with the highest malware detection accuracy to reinforce cloud security measures. Also, Zekri et al. [50] developed a DDoS detection mechanism using the C4.5 decision tree algorithm, aimed at defending against

Journal of Information Systems Engineering and Management
2022, 7(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DDoS threat. Their system achieved a detection rate of 98%, with detection performance improving in proportion to the duration of the DDoS attack.

Considering the effectiveness of individual machine learning techniques in detecting and mitigating various cloud security threats, several researchers have also explored hybrid ML approaches to further enhance detection accuracy and adaptability. Some of these are highlighted in Table 4.

Table 4: Recent Hybrid ML Models for Cloud Security

Reference	Problem or Attack Type	Proposed Technique	Results
[51]	Intrusions	Used KNN, SVM for attack detection and R-Tree for incremental learning of model.	Proven effective for intrusion detection in dynamic cloud environments with continuous learning needs
[52]	Network based attacks	Proposed a hybrid ML system using supervised learning for feature selection and unsupervised learning for clustering network threats	Improved threat classification accuracy
[53]	Intrusions	Designed a network-based threats using a combined approach of K-means clustering and SVM classification	Highlighted potential but noted limited performance of SVM in purely supervised scenarios
[54]	Anomaly Detection	Implemented an SVM-based classifier optimized using Binary and Standard Particle Swarm Optimization (BPSO/SPSO) for feature selection and parameter tuning	Achieved high detection accuracy and maintained low FARs on NSL-KDD dataset.

DISCUSSIONS

In this section, we are going to discuss the outcome of this review for each research question (RQ1 to RQ3) which would be helpful for future explorations in context of improving Cloud services security.

RQ1: Identify which security issues make CC vulnerable to attacks?

This question aims to comprehend the different requirements for cloud security and the imperative to protect server resources that are susceptible to malevolent attacks. Since cloud computing is a widely used technology, consumers can remotely access sensitive resources like network equipment, big data centres, and computing power, making it vulnerable to attacks. In the absence of countermeasures, hackers can take advantage of any weakness in a cloud device and turn it into a bot that targets defenceless devices.

As a result, the bot or compromised device turns every computer, server, and resource in the cloud ecosystem at danger. Furthermore, if the attacker manages getting into the command prompt or administration server, they can take control of multiple devices. Furthermore, insider threats pose an even greater challenge, as they originate from individuals who already have legitimate access to critical systems, making them difficult to detect using conventional security tools like firewalls [55].

Another major concern arises from inadequate access control, which can mistakenly grant permissions or extended privileges to unauthorized users. All of these problems in a cloud environment are brought on by inadequate security methods and defences.

Moreover, the negligence to regularly scan and update cloud resources, as well as failing to evaluate their ability to detect security vulnerabilities, significantly increases the likelihood of successful cyberattacks. Another critical aspect is poorly configured cloud systems often stems from inactive data encryption or poorly configured security systems or dependency of default passcodes etc. Additionally, insecure APIs represent a major security gap, typically arising from flawed authentication and authorization policies or the integration of untrusted API endpoints.

RQ2: What are the major threats faced in CC environments over time?

Based on the articles collected and condensed in Table 3 and 4, the analysis provided in this work examines and recognizes 29 different security concerns and ways of attacking in CC systems. The investigations concentrate on risks

that have surfaced over time, paying special emphasis to the ways in which hybrid ML models and machine learning (ML) have been used to counter them with one or two models of DL and Optimization based methods.
Out of the various attacks, DDoS stands out as the most heavily studied, with 9 papers proposing various ML-based to detect and mitigate this attack in Cloud systems. The second most frequent issue addressed is network intrusion, featured in around 5 articles. These studies explore intrusion detection at different layers of the cloud stack, including hypervisors and mobile cloud environments, utilizing ML models.
In contrast, several other threats were addressed in only a single case study each, indicating either emerging concerns or areas that have not yet received significant research attention. These include:

- Zero-trust access control vulnerabilities
- VB5G cloud infrastructure
- Malicious insider behaviour
- Ransomware and Android malware attacks
- APTs
- Trust violations and privacy issues

RQ3: Which ML techniques or approaches have been put forward for enhancing security in cloud systems?

This review analyzed different ML models that have been employed to mitigate various security challenges in cloud systems. These models have been applied to address a wide spectrum of threats including DDoS attacks, network intrusions, malware infections, insider threats, zero-day vulnerabilities, and unauthorized data access. Compared to traditional defence mechanisms like firewalls and IDS, ML techniques offer greater adaptability and precision because of their ability to learn from data during the training phase which allows them to identify both known and previously unseen (zero-day) attacks with higher accuracy.
Throughout this review, we observed that SVM is one of the frequently used ML model mentioned in 9 articles for detecting various threats in Cloud. As seen in Table 3 and 4, SVM has been effectively used in detecting anomalies, SQL injection, and network intrusions due to its robustness in handling high-dimensional data and binary classification tasks. Following this, RF has been used in for ransomware analysis, and API misuse identification and even for DDoS attacks.

The review also found a growing interest in hybrid models, where combinations of multiple ML/DL techniques are utilized to improve detection accuracy and resilience. Notable hybrid implementations include:

- **K-means + SVM** for hypervisor-level intrusion detection
- **BPSO-optimized SVM** for network anomaly classification
- **CNN-BiLSTM** for detecting SQL injection in SaaS layers
- **Auto-encoder + Softmax regression** for detecting APTs
- **RL-Q Matrix + VGAN** in a zero-trust VPC environment for secure job scheduling

In context of DL, auto-encoders and CNNs have been applied in cases where sequential data analysis and feature extraction are critical. These models are particularly effective for complex threat detections like APTs.

- Open Challenges

Despite the promising advancements in applying ML techniques to secure cloud computing environments, several open challenges persist that hinder the full realization of these approaches.

- One of the primary technical limitations involves the computational overhead associated with training and executing complex ML/DL models. The process of analysing large-scale cloud data often demands significant processing resources during the model training phase. As seen in [56], the integration of key generation and encryption mechanisms contributed to a noticeable spike in computational load, resulting in performance delays.
- Another pressing challenge is the limited scope of threat coverage in many of the proposed models. While a majority of recent studies, as reflected in Tables 3 and 4 of this review, focus on high-impact threats like DDoS and intrusion detection, several models fall short of addressing a broader range of attack types. This narrow focus restricts the models' real-world applicability, leaving them vulnerable to unanticipated or composite attack strategies.

- Furthermore, the lack of standardized, diverse, and up-to-date datasets that accurately reflect the dynamic and heterogeneous nature of cloud environments. Many of the reviewed case studies rely on a few publicly available datasets like NSL-KDD, CICIDS 2017, or ISCX 2012, which—while useful are often limited in scope and outdated with respect to modern cloud architectures
- Lastly, while ML learning approaches have gained traction in recent years due to their collaborative potential, they continue to grapple with fundamental issues as highlighted in [57].

CONCLUSION

This review provides a comprehensive analysis of recent advancements in cloud computing security through the lens of machine learning and deep learning. The study shows that ML models outperform traditional defence mechanisms by offering improved detection capabilities, particularly for DDos and zero-day attacks. Ml algorithms such as; SVM, RF, and KNN emerged as the most frequently applied and effective techniques across the examined case studies. However, despite their potential, these methods face challenges such as training complexity, and evolving attack patterns. Through this review, some key gaps were observed such as the absence of standardized datasets and inadequate coverage of multi-layered threats which must be addressed in future research. Overall, the integration of intelligent learning systems in cloud security holds great promise, but it requires continued innovation, collaboration, and real-time adaptability to keep pace with emerging threats.

REFRENCES

[1] Velde, V., Mandala, S. K., Vurukonda, N., & Ramesh, D. (2021). WITHDRAWN: Enterprise based data deployment inference methods in cloud infrastructure.
[2] El-Seoud, S. A., El-Sofany, H. F., Abdelfattah, M., & Mohamed, R. (2017). Big Data and Cloud Computing: Trends and Challenges. International Journal of Interactive Mobile Technologies, 11(2).
[3] Montazerolghaem, A., Yaghmaee, M. H., & Leon-Garcia, A. (2020). Green cloud multimedia networking: NFV/SDN based energy-efficient resource allocation. IEEE Transactions on Green Communications and Networking, 4(3), 873-889.
[4] Patel, H. B., & Kansara, N. (2021). Cloud computing deployment models: A comparative study. International Journal of Innovative Research in Computer Science & Technology (IJIRCST).
[5] Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57-65.
[6] Ariffin, M. A. M., Ibrahim, M. F., & Kasiran, Z. (2020). API vulnerabilities in cloud computing platform: attack and detection. International Journal of Engineering Trends and Technology, 1, 8-14.
[7] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. IEEE Access, 9, 20717-20735.
[8] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," Cluster Comput., vol. 22, pp. 949–961, Sep. 2017, doi: 10.1007/s10586-017-1117-8.
[9] Babu, M. C., & Senthilkumar, K. (2021). WITHDRAWN: WITHDRAWN: Machine learning based strategies for secure cloud.
[10] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.
[11] P. Deshpande, S. Sharma, P.S. Kumar, Security threats in cloud computing, in: International Conference on Computing, Communication & Automation, IEEE, 2015, pp. 632–636.
[12] Alsolami, E. (2018). Security threats and legal issues related to Cloud based solutions. Int. J. Comput. Sci. Netw. Secur, 18, 156-163.
[13] Barona, R., & Anita, E. M. (2017, April). A survey on data breach challenges in cloud computing security: Issues and threats. In 2017 International conference on circuit, power and computing technologies (ICCPCT) (pp. 1-8). IEEE.
[14] Nadeem, M. A. (2016). Cloud computing: security issues and challenges. Journal of Wireless Communications, 1(1), 10-15.
[15] Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of network and computer applications, 71, 11-29.

[16] Velliangiri, S., & Premalatha, J. (2017). Intrusion detection of distributed denial of service attack in cloud. Cluster Computing, 22(S5), 10615–10623.
[17] Shidaganti, G. I., Rai, S. V., Inamdar, A. S., & Rajeev, A. M. (2020). SCEF: A Model for Prevention of DDoS Attacks From the Cloud. International Journal of Cloud Applications and Computing, 10(3), 67–80.
[18] Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud. IEEE Access, 8, 181916–181929.
[19] Shaikh, A. H., & Meshram, B. B. (2020). Security Issues in Cloud Computing (pp. 63–77). Springer Singapore.
[20] Sahoo, S., Dragicevic, T., & Blaabjerg, F. (2020). Multilayer Resilience Paradigm against Cyber Attacks in DC Microgrids. IEEE Transactions on Power Electronics, 36(3), 2522–2532.
[21] Gandhi, N., Sisodiya, R., Mishra, S., Doshi, N., & Patel, J. (2021). A CNN-BiLSTM based Approach for Detection of SQL Injection Attacks. 378–383.
[22] Luo, A., Fan, W., & Huang, W. (2019, June 1). A CNN-based Approach to the Detection of SQL Injection Attacks.
[23] Abdullayeva, F. J. (2021). Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. Array, 10, 100067.
[24] Huerta, Y. A., & Lilja, D. J. (2021). Revisiting the effects of the spectre and meltdown patches using the top-down microarchitectural method and purchasing power parity theory. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 1(1), 100011.
[25] Rajasoundaran, S., Prabu, A. V., Routray, S., Kumar, S. S., Malla, P. P., Maloji, S., ... & Ghosh, U. (2021). Machine learning based deep job exploration and secure transactions in virtual private cloud systems. Computers & Security, 109, 102379.
[26] Marwan, M., Kartit, A., & Ouahmane, H. (2018). Security enhancement in healthcare cloud using machine learning. Procedia Computer Science, 127, 388-397.
[27] Kushwah, G. S., & Ranga, V. (2021). Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 105, 102260.
[28] Kumar, K. S., Nair, S. A. H., Roy, D. G., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers & Electrical Engineering, 96, 107440.
[29] Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. Journal of Information Security and Applications, 53, 102532.
[30] Li, S., Li, Y., Han, W., Du, X., Guizani, M., & Tian, Z. (2021). Malicious mining code detection based on ensemble learning in cloud computing environment. Simulation Modelling Practice and Theory, 113, 102391.
[31] Rabbani, M., Wang, Y. L., Khoshkangini, R., Jelodar, H., Zhao, R., & Hu, P. (2020). A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing. Journal of Network and Computer Applications, 151, 102507.
[32] Dey, S., Ye, Q., & Sampalli, S. (2019). A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. Information Fusion, 49, 205-215.
[33] Abdullayeva, F. J. (2021). Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. Array, 10, 100067.
[34] Cohen, A., & Nissim, N. (2018). Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Systems with Applications, 102, 158-178.
[35] Gao, X., Hu, C., Shan, C., Liu, B., Niu, Z., & Xie, H. (2020). Malware classification for the cloud via semi-supervised transfer learning. Journal of Information Security and Applications, 55, 102661.
[36] Wang, P., & Wang, Y. S. (2015). Malware behavioural detection and vaccine development by using a support vector model classifier. Journal of Computer and System Sciences, 81(6), 1012-1026.
[37] Shamsolmoali, P., & Zareapoor, M. (2014, September). Statistical-based filtering system against DDOS attacks in cloud computing. In 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1234-1239). IEEE.
[38] Rukavitsyn, A., Borisenko, K., & Shorov, A. (2017, February). Self-learning method for DDoS detection model in cloud computing. In 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 544-547). IEEE.
[39] Abusitta, A., Bellaiche, M., Dagenais, M., & Halabi, T. (2019). A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems, 98, 308-318.

[40] Sharma, V., Verma, V., & Sharma, A. (2019). Detection of DDoS attacks using machine learning in cloud computing. In Advanced Informatics for Computing Research: Third International Conference, ICAICR 2019, Shimla, India, June 15–16, 2019, Revised Selected Papers, Part II 3 (pp. 260-273). Springer Singapore.

[41] Zhu, Q. H., Tang, H., Huang, J. J., & Hou, Y. (2021). Task scheduling for multi-cloud computing subject to security and reliability constraints. IEEE/CAA Journal of Automatica Sinica, 8(4), 848-865.

[42] Yuan, J., & Yu, S. (2013). Privacy preserving back-propagation neural network learning made practical with cloud computing. IEEE Transactions on Parallel and Distributed Systems, 25(1), 212-221.

[43] Z. He, T. Zhang, and R. B. Lee, "Machine learning based DDoS attack detection from source side in cloud," in Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud), Jun. 2017, pp. 114–120, doi: 10.1109/CS Cloud.2017.58.

[44] R. Kumar, S. P. Lal, and A. Sharma, "Detecting denial of service attacks in the cloud," in Proc. IEEE 14th Int. Conf. Dependable, Autonomic Secure Comput., 14th Int. Conf. Pervas. Intell. Comput. 2nd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech), Aug. 2016.

[45] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, "A novel framework for intrusion detection in cloud," in Proc. 5th Int. Conf. Secur. Inf. Netw. (SIN), 2012, pp. 67–74.

[46] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "Trust issues that create threats for cyber attacks in cloud computing," in Proc. IEEE 17th Int. Conf. Parallel Distrib. Syst., Dec. 2011, pp. 900–905

[47] Khan, A.N.; Fan, M.Y.; Malik, A.; Memon, R.A. 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.

[48] Yuhong, L.; Yan, S.; Jungwoo, R.; Syed, R.; Athanasios, V. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J. Comput. Sci. Eng. 2015, 9, 119–133.

[49] Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci. 2019, 16, 435.

[50] Zekri, M.; El Kafhali, S.; Aboutabit, N.; Saadi, Y. DDoS attack detection using machine learning techniques in cloud computing environments. In Proceedings of the International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco, 24–26 October 2017; pp. 1–7.

[51] Xu, B., Chen, S., Zhang, H., & Wu, T. (2017, November). Incremental k-NN SVM method in intrusion detection. In 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS) (pp. 712-717). IEEE.

[52] 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.

[53] I. Aljamal, A. Tekeoğlu, K. Bekiroglu and S. Sengupta, "Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 2019, pp. 84-89

[54] Sakr, M. M., Tawfeeq, M. A., & El-Sisi, A. B. (2019). Network intrusion detection system based PSO-SVM for cloud computing. International Journal of Computer Network and Information Security, 13(3), 22.

[55] Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208.

[56] Rajasoundaran, S., Prabu, A. V., Routray, S., Kumar, S. S., Malla, P. P., Maloji, S., & Ghosh, U. (2021). Machine learning based deep job exploration and secure transactions in virtual private cloud systems. Computers & Security, 109, 102379.

[57] Sheng, V.; Zhang, J. Machine Learning with Crowdsourcing: A Brief Summary of the Past Research and Future Directions. In Proceedings of the AAAI Conference on Artificial Intelligence, Honolulu, HI, USA, 27 January–1 February 2019; pp. 9837–9843.