Article

Not peer-reviewed version

Literature Review of Machine Learning and Threat Intelligence in Cloud Security

Rrezearta Thaqi , Bujar Krasniqi , Artan Mazrekaj , Blerim Rexha *

Posted Date: 8 October 2024

doi: 10.20944/preprints202410.0512.v1

Keywords: Cloud computing; security; threat intelligence; machine learning

 doi:10.20944/preprints202410.0512.v1

Article

Literature Review of Machine Learning and Threat Intelligence in Cloud Security

Rrezearta Thaqi, Bujar Krasniqi Artan Mazrekaj and Blerim Rexha *

Faculty of Electrical and Computer Engineering, University of Prishtina
* Correspondence: blerim.rexha@uni-pr.edu

Abstract: Cloud computing has transformed IT services by making them more scalable and cost-effective. However, this shift has also introduced new security challenges that traditional methods are finding hard to tackle. This review paper looks at how combining machine learning (ML) with dynamic threat intelligence can improve cloud security — an approach that hasn't been widely explored yet. By reviewing recent studies, we show that ML and threat intelligence can do more than just detect known threats. They can also adapt to new and evolving ones, making cloud systems much secure against cyber attacks. Our analysis highlights how this combined approach provides better protection and flexibility. We also identify some important gaps in the current research and suggest areas for future study to make these security systems even more effective. This review aims to provide useful insights for researchers, helping to build more proactive cloud security strategies.

Keywords: cloud computing; security; threat intelligence; machine learning

1. Introduction

Earlier, IT organizations utilized computing models, specifically on-premise technologies, in order to acquire the necessary services. However, despite the fact that on-premise technologies offer a high level of security and complete control, IT organizations encounter numerous challenges pertaining to cost, scalability, and backup data [1]. In recent years, there has been a surge in the popularity and recognition of cloud computing, which is now being adopted by enterprises as an alternative to on-premise technologies for service provision. Cloud computing, a technology established by a third party, facilitates the delivery of various services and resources to customers through the utilization of the internet. Enterprises simply engage with the service provider to obtain the required services and access to resources. The array of services offered by cloud computing to its customers encompasses computing resources, data storage, networking techniques, and software applications [2]. [3] shows that a big part of organizations using cloud are concerned and more oriented on working to improve cloud security. Figure 1 presents this level of concerning on percentage.

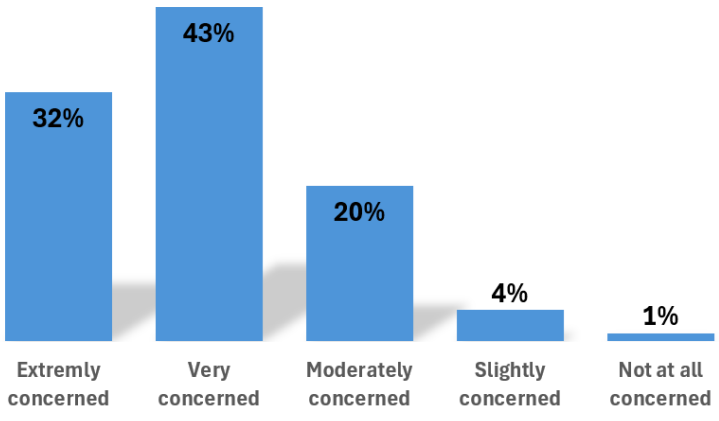

Figure 1. The percentage of concerning of organizations for cloud security [3].

 doi:10.20944/preprints202410.0512.v1

On-demand self-service, pay-per-use resources, resource mobile-access, resource pooling, virtualization, and rapid elasticity constitute a subset of the properties associated with cloud computing [4]. When compared to on-premise techniques, cloud computing offers several advantages, such as high scalability, low cost, low maintenance, unlimited storage capacity, and the ability to access resources via the Internet from any location [1]. However, cloud computing also presents certain disadvantages, including compatibility issues between cloud systems, the need for high-speed connections, and the potential for data disclosure or loss. Security emerges as a paramount concern within the realm of cloud computing, as it impedes the establishment of a safe and secure environment [2]. The cloud serves as a repository for data with varying levels of sensitivity, ranging from public to internal-only, confidential, and restricted. Furthermore, it effectively caters to customers' needs by providing computation resources that operate continuously.

One of the biggest concerns for cloud is its security. As cloud is a place that stores sensitive data, it is vulnerable to risks and threats posed by attackers who attempt to exploit any weakness in the system in order to undermine the goals of security, including confidentiality, integrity, and availability. For instance, the cloud environment is susceptible to attacks such as malicious insiders, phishing, fraud, signature wrapping attacks, denial of service attacks, insecure interfaces, and various others [5]. Furthermore, the tools employed by hackers today are increasingly advanced and effective. Additionally, the large volumes of data stored or exchanged between the cloud and consumers have escalated, thereby increasing the likelihood of introducing new or undetectable malware [6]. Consequently, the traditional countermeasures and techniques utilized to safeguard the cloud environment, identify malware and anomalies, and protect privacy are inadequate. Therefore, more effective techniques must be employed to enhance the security of cloud computing. As it is seen in Figure 2, there is a growing trend towards cloud security, highlighting the growing significance of cloud solutions today.

Figure 2. The trend of the 'cloud security' term from Google Trends.

Machine learning with threat intelligence has gained significant popularity in recent years and is employed across various domains, including natural language processing, computer vision, data analysis, speech recognition, and predictive analysis, among others. The usage of machine learning techniques in cloud computing applications has also emerged as a recent trend [7]. Notably, one of the primary applications of machine learning in this context is enhancing the security of cloud computing. Compared to traditional methods like firewalls, intrusion detection systems (IDSs), and anti-virus software, machine learning presents a highly efficient approach for securing cloud computing. This is primarily due to its ability to analyze vast amounts of data flow, identify vulnerabilities, threats, and attacks within the cloud environment (including unknown attacks), and leverage historical information and extensive datasets [8]. Additionally, within cloud computing, machine learning techniques are employed to ensure resource availability, preserve equipment reliability, maintain system quality, and extend the lifespan of the equipment. These strategies effectively mitigate service outages and data loss [9]. Known as proactive maintenance techniques, machine learning-based maintenance approaches utilize pre-trained data containing the system's quality characteristics and future states to predict system failures before they occur [10].

Yaara Shriki, a researcher in the field of security, predicted that in the year 2024, the integration of artificial intelligence and machine learning in threat intelligence within cloud security will bring a significant transformation in the identification and mitigation of cyber threats [11].

 doi:10.20944/preprints202410.0512.v1

Although various reviews have focused either on machine learning techniques or on threat intelligence separately, little attention has been given to how these two approaches can be combined in the development of a more dynamic and adaptive cloud security framework. This review therefore seeks to bridge this gap by the analysis of the synergistic potentials of these technologies in combating both known and emerging threats in cloud environments.

The paper is structured as follows: Section 2 shows the methodology used for the research; Section 3 dives into the background of cloud security and cloud computing models; Section 4 outlines various security threats facing cloud environments; Section 5 explores the application of supervised and unsupervised learning algorithms and the threat intelligence role in detecting cloud security threats; Section 6 reviews existing literature on cloud security, machine learning, and threat intelligence; Section 7 shows the results gotten from the papers analysis; Section 8 discusses the results and suggests future research directions; Section 9 wraps up the paper with a conclusion.

2. Methodology

This section outlines the process of identification, selection, and analysis that was undertaken for identifying relevant research papers for this review.

2.1. The Searching Process

The study uses different databases such as IEEE Xplore, ScienceDirect, Google Scholar, etc. Hence, in an effort to capture the wide spectrum of the topic, a thorough search was conducted by combining keywords and Boolean operators. Key strings were combined with the logical Boolean operator "AND" and "OR". These words are included in the search strings that have been used to conduct literature reviews: "cloud security", "machine learning", "cyber threat intelligence", "cybersecurity in cloud computing", "dynamic threat intelligence". The search was confined to finding relevant peer-reviewed journal articles, conference papers, and high-quality technical reports that were published the last 5 years to ensure that most of the current trends in the subject under discussion are captured.

2.2. Data Extraction and Synthesis

A standard data extraction form was used to extract information from selected studies, which included:

Features of the study: Authors, publication year, and title.

Methodology: Machine learning technique adopted, type of integrated threat intelligence, and cloud security focus area.

Evaluation metrics: Performance metrics such as accuracy, precision, recall, F1-score, and any other metrics relevant to the effectiveness of the proposed methods.

Key findings: Main results and conclusions drawn from the study.

Data extracted were synthesised qualitatively to identify common themes, methodologies, and research gaps. Where appropriate, summary of quantitative data was done using descriptive statistics.

3. Background

Cloud computing is a system that allows users or data owners to remotely store and access their data from anywhere in the world. This technology eliminates the need for users to store and manage their data locally by utilizing a shared pool of programmable resources. With recent advancements, cloud computing can offer innovative and technologically compatible services and products to a wide range of users, with different pricing options available when needed. By pooling together various resources, cloud computing ensures immediate access and availability of resources based on user demand. The cloud provider ensures efficient utilization of resources, providing flexibility and a suitable solution for end-users. Consequently, cloud computing is now being utilized in almost every aspect of business and personal situations, leading to an increased demand for cloud services.

 doi:10.20944/preprints202410.0512.v1

However, the use of shared resources by multiple users on the same network poses risks to sensitive information being transferred [12].

Today's cyber criminals take advantage of the cloud computing services to perform criminal acts in an environment that is decentralized. By utilizing more powerful computational tools provided by cloud services, these cyber criminals perform their attacks within a short time frame. Within the cloud environment, security threats come from internal sources within the organization as well as from the external enemies of the organization.

The growing usage of cloud computing in recent years has altered the way businesses handle and store data. The cloud has various advantages, including scalability, cost-effectiveness, and flexibility. However, with the growing reliance on cloud services, implementing adequate security measures is critical [13].

In the context of cloud services, the processing and storage of sensitive data pose additional challenges in terms of cybersecurity. Moreover, it is essential to protect user data and proprietary information in order to uphold trust, adhere to privacy regulations, and prevent potential consequences. Additionally, the dynamic and scalable nature of cloud services brings up unique difficulties in maintaining a consistent security posture. While scalability is advantageous, it requires careful consideration of security implications. The notion that the distributed nature of cloud services gives rise to specific cybersecurity challenges is substantiated by examining the types of attacks they are susceptible to [14].

According to [15], a lot of the security issues we run into with cloud computing stem from weak spots in the building blocks and technologies of cloud architecture. Further, the author say that this includes things like flaws in how the internet communicates, web services, the structure of web-based services, browsers, the tech behind creating virtual spaces (like virtualization and hypervisors), the way different users share the same resources (multi-tenancy), the software itself, virtual machines, and the platforms we use to manage all these services by ourselves. On top of that, because cloud services keep our data somewhere else, not directly under our control, it's pretty common for people to feel uneasy about the potential of losing grip on their personal or sensitive information.

At the other hand, the authors in [16], say that the more we rely on the cloud, the old-school security vulnerabilities we've always worried about become even scarier, because everything's more exposed. And on top of that, we're facing brand new kinds of cloud-specific threats, like the risk of someone hacking into cloud storage.

3.1. Cloud Computing Models

In cloud computing, there are four diverse types of delivery models supported: private cloud, public cloud, hybrid cloud, and community cloud [17,18].

3.1.1. Private Cloud

Private cloud offers a combination of cloud computing benefits such as elasticity, scalability, and ease of service delivery, along with access control, security, and resource customization similar to on-premises infrastructure.

Many organizations prefer private cloud to public cloud due to regulatory compliance requirements, especially when dealing with sensitive data like confidential documents, intellectual property, or medical records.

By constructing private cloud architecture based on cloud native principles, a company allows itself the flexibility to transition workloads to public cloud or operate within a hybrid cloud environment when the time is right [19].

 doi:10.20944/preprints202410.0512.v1

3.1.2. Public Cloud

The public cloud infrastructure is accessible to the broader public or a large-scale industrial entity that offers cloud services. Within the public cloud, resources can be accessed via the internet with the pay-per-usage model. Public cloud delivers services based on the users' capacity requirements [20].

In public cloud, it's not possible to know about the data residency. Reliability can also be an issue in public cloud computing [21].

3.1.3. Hybrid Cloud

Hybrid cloud is a combination of computing environments where applications run on public and private clouds, as well as on-premises data centers or edge locations. It is widely used today as few rely solely on one public cloud.

Migrating workloads between different cloud environments is made possible by hybrid cloud solutions, allowing for more adaptable setups based on specific business needs. Organizations opt for hybrid cloud platforms to lower costs, reduce risk, and enhance capabilities for digital transformation efforts.

The hybrid cloud approach is prevalent in modern infrastructure setups. Cloud migrations often result in hybrid cloud implementations as organizations transition applications and data gradually. This setup enables the use of on-premises services alongside the flexible storage and access options provided by public cloud providers [22].

Figure 3 presents a detailed example of a hybrid cloud model, showing how public and private cloud infrastructures can be effectively integrated to leverage the strengths of both environments for enhanced flexibility and security for a healthcare cloud system.

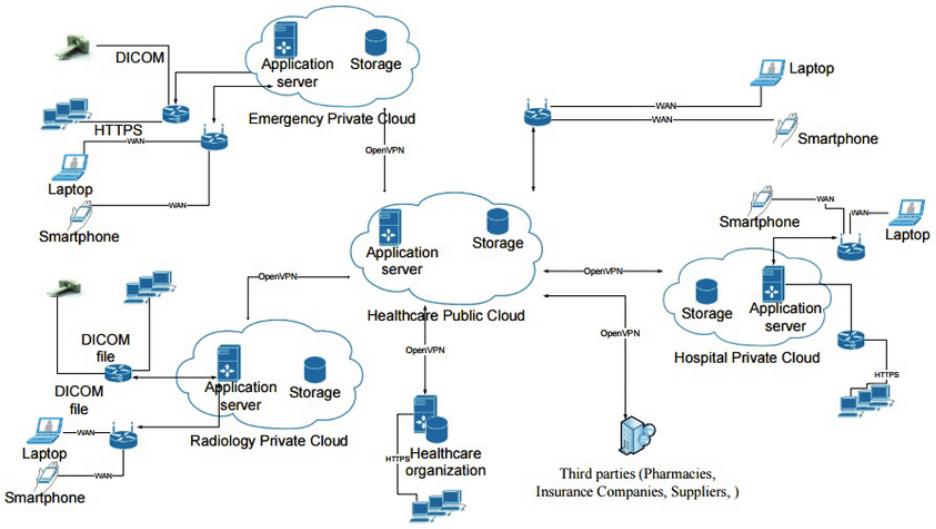

Figure 3. An example of a hybrid cloud model [23].

3.1.4. Community Cloud

A community cloud is described as a cloud infrastructure where various organizations pool resources and services according to shared operational and regulatory needs.

Organizations part of a community cloud have similar business needs, often centered around shared data, services, or industry regulations. These organizations are typically from the same industry or branches of the same organization. Essentially, a community cloud is a unified system that leverages features from multiple clouds to cater to a specific industry. Figure 4 shows an example of a community cloud model, designed for shared use by two organizations. This setup allows both entities to benefit from cost savings and enhanced security through a collectively managed and specifically tailored cloud environment.

 doi:10.20944/preprints202410.0512.v1

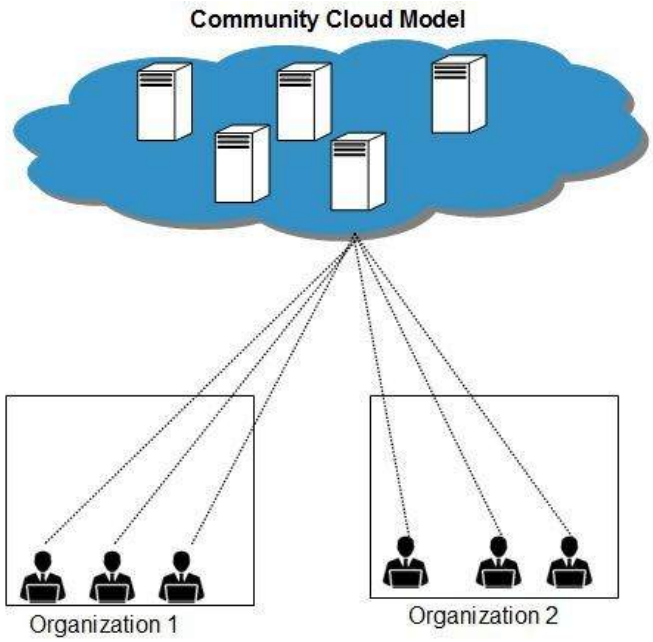

Figure 4. An example of a community cloud model [24].

In order to establish a community cloud, organizations can opt to host their own data centers and divide the costs and responsibilities. This could be on-premise within a member's current infrastructure or at partner facilities [25].

4. Cloud Security Threats and Attacks

Nowadays there are many types of threats in cloud environments and day by day there are becoming more dangerous and unstoppable. There is a slight difference between a threat and an attack. According to [26], a threat is anything that can lead to an attack, including viruses, trojans and back doors that can help hackers for attacks. Now, all the threats mentioned can lead to different kinds of attacks. Even if it is undeniable that cloud computing provides a lot of resources over the internet, it still can face both inside and outside attacks.

In their 2024 report, CrowdStrike [27] unveiled that attackers are now more frequently exploiting stolen identity credentials. This strategy targets weaknesses within cloud environments, aiming to enhance the discreetness, rapidity, and severity of their cyber attacks. With more workloads, it becomes critical for the cloud to discover, monitor, and remediate service misconfigurations, malware, and inappropriate access and privileges.

In some of the recent studies, a big importance has been given to threats such as data breaches, data loss and corruption, account hijacking, hypervisor threats, DDoS, etc.

The authors in [28] classify the cloud security threats into six categories, such as: network security, virtualization and hypervisor security, identity and access management, data and storage security, governance, and legal and compliance issues.

According to [29], common threats in cloud computing include data breaches, which can result in unauthorized access to sensitive information stored in the cloud. This can lead to a loss of confidentiality and privacy for individuals and organizations, as well as potential legal and financial implications. More on, they state that another common threat is the risk of data loss or corruption, which can occur due to factors such as hardware failure, human error, or malicious attacks. In addition, cloud computing environments are vulnerable to distributed denial of service (DDoS) attacks, which can disrupt services and cause downtime for users. It is essential for organizations to implement robust security measures to protect against these threats and safeguard their data in the cloud.

This section will briefly explore some of the most popular ones.

 doi:10.20944/preprints202410.0512.v1

4.1. Data Breaches

The fear of experiencing a data breach is a major concern for anyone using cloud services. Essentially, a data breach happens when protected or confidential information, like for example, credit card, is stolen, or used without authorization. Unfortunately, there's no single method guaranteed to prevent data breaches entirely. The best approach to minimize the risk involves sticking to fundamental security practices. This means regularly performing vulnerability and penetration tests, creating strong passwords, and timely updating software patches across all systems. Additionally, if an unauthorized entry does occur, having encryption in place can stop cybercriminals from getting their hands on the actual data [30].

4.2. Data Loss and Corruption

Data loss prevention (DLP) is a key security tactic in today's cloud computing age. DLP tools safeguard important data to prevent unauthorized sharing beyond specified trust boundaries [31].

Data corruption often leads to data being lost forever, but protecting against data breaches tends to be prioritized, even though both can have serious effects. According to Statista [32], data loss and leakage (69%), and data privacy/confidentiality (66%) are the top cloud security concerns followed by accidental exposure of credentials (44%).

4.3. Account Hijacking

Account hijacking is when a hacker or another unauthorized user takes over someone's online account, often targeting financial ones. It's become one of the most significant problems for consumers and organizations alike, especially those relying on cloud-based communication. Victims of account hijacking face severe risks, including the potential for bankruptcy and the loss of confidential information. Once an account is taken over, there's a real risk it may be irretrievably lost, leaving the original owner without any way to regain access. Even if the account is recovered, it may not be returned to its original state; settings might be altered, and the account could have been used for unwanted or false advertising [33]. According to [34], these days, taking over someone's account is a serious form of attack, with attackers constantly attempting to steal login details from various cloud service users.

4.4. Hypervisor Threats

A virtual machine (VM) is one of the domains in the cloud that can easily be compromised by such threats because of its inherent vulnerabilities [35]. A hypervisor is like the manager of a virtual space, running several virtual machines (VMs) and applications simultaneously on one computer while keeping them separate from each other. Despite being designed for safety and reliability, hypervisors can still be prime targets for attacks because of the extensive control they have over all the VMs. If an attacker manages to take control of a hypervisor, they essentially get the keys to the kingdom - they can access and exploit all the virtual machines and the data within them as they please [36].

In their paper [37], the authors provide an in-depth analysis of various attack vectors targeting virtual machines (VMs). These attacks are systematically categorized and illustrated in Figure 5, offering a comprehensive visual overview of the security vulnerabilities prevalent in VM and cloud environments.

 doi:10.20944/preprints202410.0512.v1

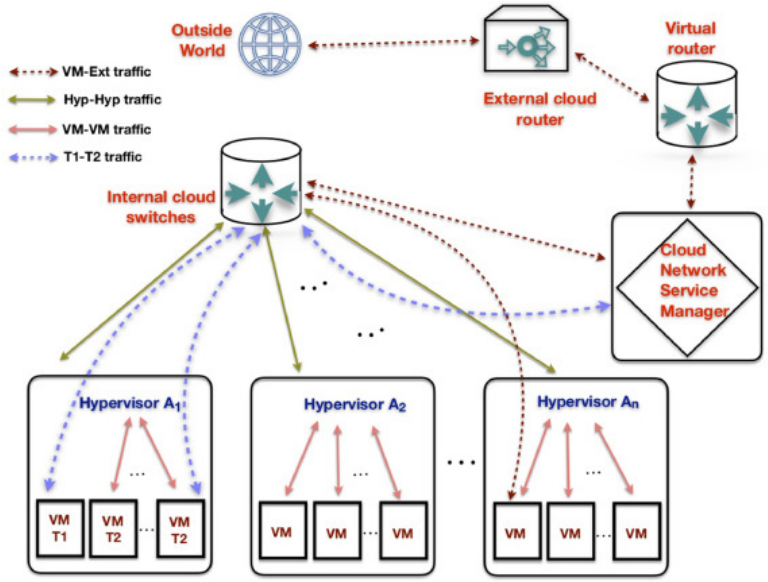

Figure 5. Network flows in a cloud environment in VMs [37].

4.5. Distributed Denial of Service (DDoS)

DDoS is among the most infamous and popular forms of cloud attacks, as it has the potential to disrupt services, degrade user experience, and result in significant financial losses that may render businesses unsustainable when utilizing cloud computing. During a DDoS attack, the attacker's goal is to overwhelm network infrastructure, capacity, or computing resources by blocking them with requests. This compromises the functionality of cloud services and weakens their ability to distinguish the legitimate users [38]. Figure 6 shows a scenario of a Distributed Denial of Service (DDoS) attack within a cloud environment, illustrating the attack pathways and potential impact points on cloud infrastructure. This visual representation also shows the complexity and scale of DDoS attacks targeting cloud services.

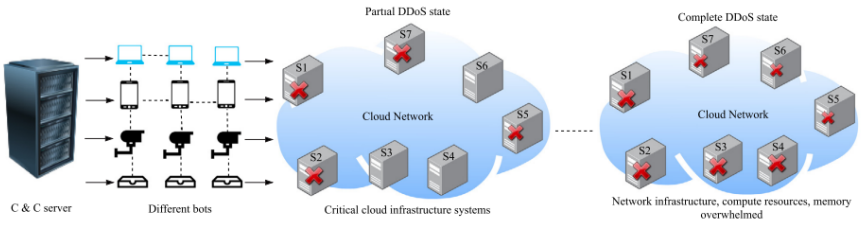

Figure 6. Scenario of DDoS attacks in cloud [38]

DDoS attacks is different when they target cloud environments compared to traditional networks. Sure, they both can knock services offline, lead to different kind of losses, and rack up costs in fighting off the attack. But in the cloud, the fallout includes some unique issues. There's the extra money burned through when systems automatically scale up to try and handle the attack, not to mention the additional power that is needed during the process. There's also the ripple effect on other parts of the cloud infrastructure, the hassle of moving data and services around to dodge the attack, and the potential trouble for other virtual machines that happen to be sharing the same physical space. Essentially, in the cloud, DDoS attacks can spiral into what's known as an Economic Denial of Sustainability (EDoS) attack, where the financial strain becomes just too much to handle [39].

5. Common Machine Learning Techniques Used in Cloud Attacks Detection

The common techniques in Machine Learning are supervised and unsupervised learning. Figure 7 shows the growth over time in the number of publications in classification/supervised, cluster-

 doi:10.20944/preprints202410.0512.v1

ing/unsupervised and feature selection. The researchers have made great efforts in developing advanced supervised classification approaches—compared to unsupervised classification and feature selection approaches [40].

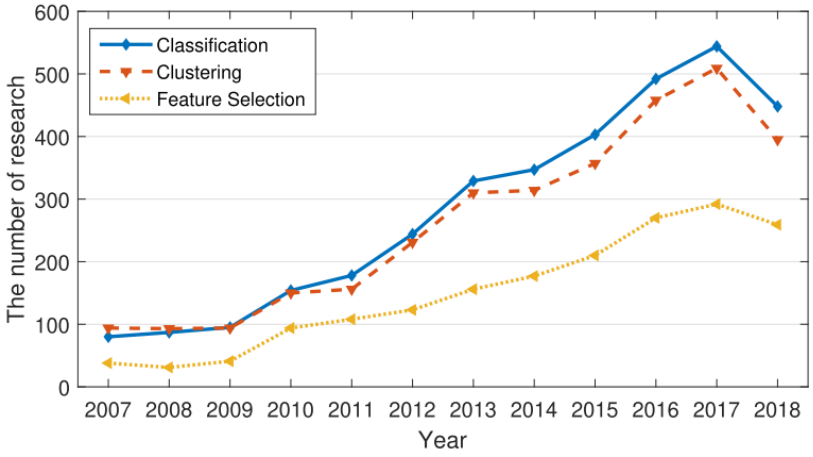

Figure 7. Evolution of IDS schemes based on machine learning approaches (between 2007-2018 and ongoing) [40].

5.1. Supervised and Unsupervised Learning Algorithms

Supervised Algorithms are often used in IDS systems. An overview of the practical implementation of the IDS approach is illustrated in Figure 8. These systems typically involve five primary steps: (A) data collection, (B) feature extraction and selection, (C) tagging, (D) training, and (E) anomaly detection. The data collection phase is the initial step where input data is gathered, such as event logs, system states, network traffic traces, or Net-flow data from a network monitor [41].

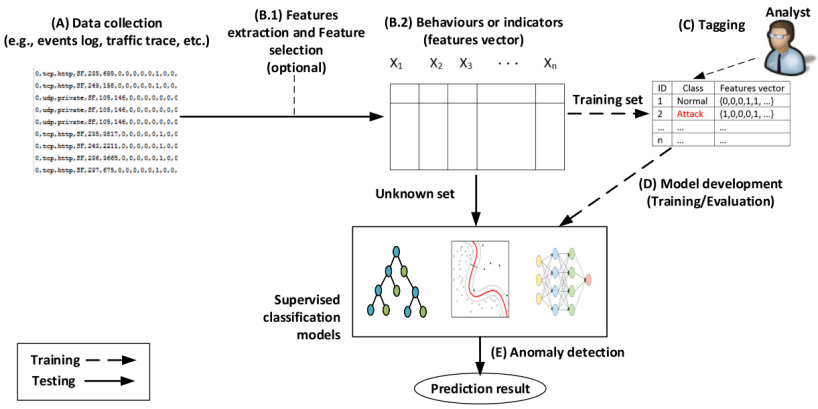

Figure 8. The process of the supervised learning-based IDS approach [40].

Supervised Learning algorithms require a labeled dataset to process different operations.

According to [42], the most preferred algorithm of supervised learning to detect attacks in cloud environments in Decision Trees.

At the other hand, unsupervised learning algorithms does not require a labeled dataset. According to [43], the algorithms in this category aim to identify natural patterns already present in the training dataset. Some typical instances are clustering algorithms and feature selection methods like Principal Component Analysis (PCA). Clustering algorithms, such as K-Nearest Neighbor (KNN), work towards grouping training examples based on the similarity of their features.

In their paper, the authors in [44], proved that the Naïve Bayes classifier, enhanced by an auto-encoder for feature selection, is the most effective unsupervised learning algorithm for anomaly detection in cloud environments.

 doi:10.20944/preprints202410.0512.v1

5.2. Threat Intelligence

Data is considered the most valuable tool that an organization can have today. This is because different organizations across various sectors rely on data to gain insights and identify meaningful patterns using data analytic engines. Machine Learning (ML) has various intelligent algorithms that are capable of extracting and acquiring informations from historical data to provide insights for data prediction or classification [45]. Consequently, ML capabilities have been integrated into threat intelligence.

Intelligence is a composite of data, information, and knowledge, which can be characterized as the interpretation of data based on evidence, collected on or against the goals, motives, tactics and techniques. Threat refers to a collection of conditions and factors that have the potential to create an environment that violates the assets of an organization, where intelligence can be the information that can be utilized to alter outcomes. Intelligence can also be a specific type of information derived from different sources, such as IP addresses, usernames, passwords, etc. When an attack event originates from an IP address, it becomes crucial to acquire knowledge about that IP address. Cyber Threat Intelligence encompasses awareness of cyber threats and the acquisition of relevant, valuable, and available information, which enables the prevention or mitigation of cyber attacks [46].

Cyber Threat Intelligence (CTI) has the potential to play a crucial role in guiding the behavior of an organization in the prevention, detection, and response to cyber-attacks. CTI can contribute to prevention efforts by notifying organizations about vulnerabilities that may be taken advantage of by particular threat actors who possess the means, motivation, and capability to target the company. Additionally, CTI can aid in the detection of cyber attacks by instructing intrusion detection systems to identify patterns of exploitation associated with specific threat actors. Furthermore, CTI can effectively direct the response to cyber attacks by providing a precise defense strategy [47]

In cyber threat intelligence there is a concept known as cyber threat attribution. Cyber threat attribution refers to the knowledge of identifying the individual or organization responsible for an attack. The attacker can have different profiles and possess various attributes [48]. Moreover, according to [49] there are different levels of attribution, as illustrated in Figure 9. The initial level involves understanding the tools, tactics, techniques, etc employed by the attacker, which serves as the first step in identifying the tools utilized. The subsequent level pertains to discerning the country associated with the attack, and finally, the most crucial level entails identifying the individual responsible for conducting the attack.

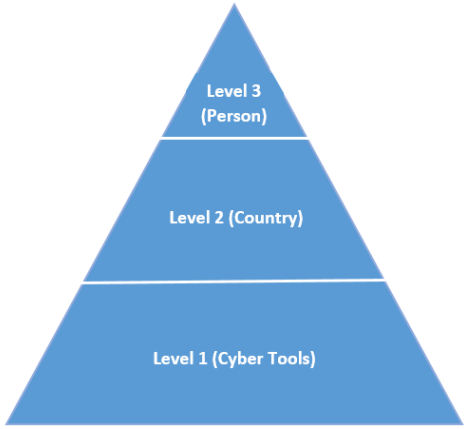

Figure 9. Levels of attributes in cyber threat intelligence [49].

According to [50], there are four types of threat intelligence:

1. Tactical Threat Intelligence is centered around the detection and recognition of indicators of compromise in order to promptly address and minimize potential risks [51]. Its purpose is to provide organizations with information regarding immediate threats, such as newly developed malware or

 doi:10.20944/preprints202410.0512.v1

phishing methods. By studying tactical threat intelligence, businesses can enhance their security systems to safeguard against the most recent threats, thereby ensuring the protection of their infrastructure in the short term.

2. Operational Threat Intelligence centers around the tactics, techniques, and procedures utilized by threat actors and offers a more comprehensive understanding of the threat landscape. This type of intelligence provides valuable insights into the behaviors and methods of cybercriminals, enabling businesses to anticipate and prepare for potential attacks. It also offers contextual information, such as the motivations behind a potential attack or the past activities of the threat actor, allowing businesses to tailor their defense and response strategies accordingly [50].

3. Strategic Threat Intelligence takes a broader perspective and delves into the larger context. It provides insights into long-term trends and emerging threats in the cybersecurity realm. This type of intelligence aids businesses in comprehending how factors at a higher level, such as technological advancements, legal changes, or geopolitical shifts, can impact cyber threats. By utilizing strategic threat intelligence, businesses can plan their long-term cybersecurity strategies, making informed decisions on where to invest resources and how to adapt as the threat landscape evolves [50].

4. Technical Threat Intelligence, which is primarily data-centric, furnishes information regarding malicious indicators, including IP addresses, domains, URLs, and malware hashes associated with threat actors. Firewalls, intrusion detection systems, and antivirus software rely on technical threat intelligence to identify and block known threats [52]. This form of intelligence enables businesses to swiftly identify and neutralize threats, thereby reducing the window of opportunity for cybercriminals to inflict damage [50].

6. Related Literature Review

The reason why machine learning and threat intelligence methods are better than traditional methods for cloud security is that they offer a more effective approach to malware detection and prevention of them [53]. Traditional security systems are ineffective in identifying security attacks comparing with the modern solutions, while machine learning models have proven effective in detecting and mitigating cyber attacks [54]. Machine learning can help in identifying vulnerabilities and new types of threats that traditional systems may not be able to detect as shown also in papers [55] [56] through predictions. By analyzing large amounts of data and building data-driven models, machine learning can enhance the security of cloud systems and provide better defense mechanisms also with the help of threat intelligence sources.

Most of the papers have considered the use of machine learning (ML) and cyber threat intelligence (CTI) to address the cloud security challenges. For instance, the authors in [57] address significant challenges in cloud security, particularly in the context of dynamic cloud environments characterized by resource sharing, outsourcing, and multi-tenancy. They highlight the limitations of traditional cloud security mechanisms in accurately detecting new or unknown attacks. To overcome these challenges, the authors propose an innovative security solution employing transfer learning techniques. The results of the paper demonstrated that this approach effectively reduces the workload of repeated attacks and maintains qualitative performance.

While the use of transfer learning addresses some detection challenges, the ability to convert real-time threat data into actionable intelligence is equally crucial, as demonstrated [58]. The authors highlight the limitations of traditional heuristic and signature-based security systems in addressing the dynamic, resilient, and complex nature of new-generation cyber threats. The study underscores the necessity of gathering and converting real-time cyber threat information into actionable Cyber Threat Intelligence (CTI) for preemptive attack mitigation and rapid response. The paper concludes by identifying current challenges and future research directions in CTI mining, aiming to broaden the scope and efficacy of cybersecurity strategies, particularly in the context of cloud environments.

In addition to addressing external threats, internal risks such as insider attacks pose significant challenges. To tackle this, researchers have developed systems like the one in [59]. The research

 doi:10.20944/preprints202410.0512.v1

proposes a machine learning-based system for detecting and classifying insider threats, focusing on identifying anomalies and security issues related to privilege escalation. The study employs ensemble learning techniques to enhance prediction performance and address the need for improved security systems capable of classifying and predicting insider attacks more effectively and efficiently. The research identifies LightGBM as the most effective algorithm, providing the highest accuracy (97%), compared to the other algorithms.

Beyond managing insider threats, enhancing anomaly detection remains a critical focus area, as explored in studies that utilize various machine learning techniques such as in [60]. A key focus of the paper is on exploring various machine learning algorithms suitable for anomaly detection in cloud environments. It delves into the specifics of algorithms like k-means clustering, Support Vector Machines (SVMs), and autoencoders, discussing their strengths and applications in enhancing cloud security. Overall, the paper underscores the importance of machine learning-powered anomaly detection in protecting valuable data and maintaining the integrity of cloud environments.

Despite these advancements in anomaly detection, the quality of threat intelligence data itself plays a pivotal role in security effectiveness. Improving this quality has been the focus of the authors in [61]. A significant issue they highlight is the quality of CTI, where inaccurate, incomplete, or outdated information leads to reactive measures, hardly different from traditional security methods. However, they also recognize that high-quality threat intelligence can substantially improve incident response times. To tackle these challenges, they propose a methodology for enhancing the quality of CTI. This methodology involves an Indicator of Compromise enrichment process, designed to refine CTI quality.

Beyond improving data quality, visualizing and analyzing vast amounts of threat intelligence data is another challenge. To address this, researchers in [62] have worked on enhancing the analysis and visualization of Cyber Threat Intelligence (CTI). The study addresses the challenge of processing and effectively utilizing vast, often unstructured CTI data. The research involves machine learning models to train on attack patterns, also known as Tactics, Techniques, and Procedures (TTPs). The results demonstrated the effectiveness of the proposed approach, enabling analysts to analyze CTI data and predict cyber threats with an accuracy of 86%.

While visualization aids in better understanding threats, detecting malicious activities by legitimate users requires sophisticated models, such as the Deep Belief Networks used in [63].The study specifically addresses the challenge of identifying malicious activities by legitimate users within cloud systems. Employing a Deep Belief Neural Network (DBN), a form of deep learning, the research aims to train on nuanced user interaction behaviors to identify potential insider threats. The results of the study are significant, with the proposed DBN model demonstrating high accuracy and F-measure scores, markedly outperforming existing methods. The system achieved an accuracy rate of 99% and an F-score of 98%, underscoring its efficiency in detecting malicious cloud users.

As cloud security extends into IoT environments, the sharing and scalability of threat intelligence become critical, which is why a hybrid cloud-based model has been suggested in [64]. The paper acknowledges the challenges in implementing CTI for individuals and organizations, particularly due to constraints such as time, capability, and cost. Therefore, the research emphasizes the need for a reliable, scalable, and high-speed CTI sharing platform. The study involves a careful analysis of various CTI sharing deployment models: private cloud, public cloud, hybrid cloud, and on-premises. After evaluating these models, the research suggests the hybrid cloud-based deployment model as the most convenient solution for CTI sharing.

To further enhance security in cloud systems, integrating innovative machine learning models, like the combination of IPCA and IHNN, offers promising results, as shown in [65]. This approach aims to address the complexities of existing machine-learning-based detection methodologies, which often suffer from issues like overfitting and high time consumption. The proposed framework encompasses preprocessing, normalization, feature extraction, optimization, and prediction phases. Using popular

 doi:10.20944/preprints202410.0512.v1

datasets such as NSL-KDD, BoT-IoT, KDD Cup'99, and CICIDS 2017 for implementation, the system demonstrates improved detection accuracy and F1-scores, outperforming other security models.

At the other hand, the paper in [66] discusses the integration of Internet of Things (IoT) technologies in Maritime Transportation Systems (MTS), highlighting the resulting cybersecurity challenges. To address these, it introduces DLTIF, an automated framework for modeling and identifying cyber threats in IoT-enabled MTS. DLTIF comprises three components: Deep Feature Extractor (DFE), CTI-driven Detection (CTIDD), and CTI-Attack Type Identification (CTIATI). DFE analyzes IoT-enabled MTS network patterns, CTIDD focuses on threat detection, and CTIATI helps identify specific threat types. The framework achieves up to 99% accuracy, surpassing traditional and contemporary approaches in threat intelligence and detection.

Meanwhile, addressing threats like DDoS attacks, particularly during the pandemic, has highlighted the need for more robust detection mechanisms, as explored by the authors in [67]. The paper identifies that standard detection systems have become ineffective against novel DDoS attacks due to the increased volume of data generated and stored. To tackle this challenge, the study focuses on employing data fusion applications alongside machine learning classifiers to enhance the security of cloud services and facilitate the detection of DDoS attacks. The findings of the study reveal that the decision tree model is the most effective, outperforming other methods in classifying cloud DDoS attacks.

In addition to attack detection, integrating various data sources to enrich threat intelligence is crucial. The use of a cybersecurity knowledge graph, as proposed by the authors in [68] focuses on integrating malware behavior data with Cyber Threat Intelligence (CTI). This methodology involves collecting and analyzing malware samples in controlled environments and then integrating this behavioral data into the CKG. This integration enables more effective correlation and validation of information from CTI sources, enriching the representations of malware threats and enhancing the reasoning capabilities of CKGs. The paper's contribution lies in its novel approach to improving the identification and understanding of malware behaviors, aiding cybersecurity professionals in threat detection and analysis.

While innovative integration approaches show promise, a comprehensive review of existing machine learning techniques provides valuable context on current capabilities and limitations, as seen in [69]. It includes a taxonomy of attacks, explores the effectiveness of machine learning (ML) and deep learning (DL) techniques in countering these threats, and discusses the limitations of traditional security methods. The study's results, derived from analyzing forty-two case studies, provide valuable insights into the current state and challenges of cloud security, highlighting the significance of ML and DL in enhancing cloud defense mechanisms.

Building on this review, recent research has tested the effectiveness of specific ML algorithms for cloud security, achieving remarkable results in areas like in paper [42]. In this paper authors have presented an effective approach for detecting dy kinds of attacks in a cloud environment: DDoS and MitC. They used four kinds of machine learning algorithms to find which is the best algorithm to then be used to detect the two kinds of the attacks. The parameters used to train the models were the number of packets per second, network bits and other elements of the network traffic. They achieved an accuracy of 100%.

For more complex environments, such as energy clouds, a tailored framework is necessary. The CTI framework proposed by the authors in [70] is designed for efficient threat detection and incident response by integrating different layers of the energy cloud system. The results of the research indicate the framework's effectiveness in detecting cyber attacks, as evidenced by its performance in a simulated energy cloud environment. The framework achieved notable scores in macro-F1 and micro-F1 metrics, underscoring its practical efficacy in responding to and managing cyber threats in the context of energy cloud platforms.

A broader view of recent developments in threat intelligence and their application in organizational contexts is offered in [71]. This review focuses on how CTI can enhance organizational

 doi:10.20944/preprints202410.0512.v1

cybersecurity by identifying, analyzing, and distributing information about potential cyber risks. The study outlines a framework comprising a knowledge base, detection models, and visualization dashboards for effective CTI implementation in organizations. This framework includes behavior-based, signature-based, and anomaly-based detection models, along with information resources on potential threats and vulnerabilities. The visualization dashboard offers an overview of key cyber threat metrics.

However, integrating threat intelligence into established cybersecurity frameworks remains challenging, as highlighted by the authors in [72]. The paper conducts a critical review of cyber threat intelligence frameworks, focusing on their architecture and application in the cybersecurity field. It examines the role and limitations of established cybersecurity frameworks, such as the Pyramid of Pain, MITRE ATTACK, Cyber Kill Chain, and The Diamond Model of Intrusion Analysis, particularly in the context of cyber threat intelligence analysis. The research identifies a gap in these frameworks: they do not specifically address the execution of activities for harnessing cyber threat intelligence data, as they were not originally designed for this purpose.

Expanding the application of threat intelligence, studies have also explored its use in detecting specific threats, such as phishing, by utilizing multi-modal approaches like in [73]. They present a multi-modal hierarchical attention model (MMHAM) that addresses the limitations of existing methods by incorporating three major modalities of website content: URLs, textual information, and visual design. Threat intelligence enhances phishing detection and offers interpretability, allowing for actionable phishing threat intelligence.

Lastly, the unique security needs of critical infrastructures like SCADA networks require continuous improvements in detection systems, as discussed in [74]. The research doesn't present empirical results but instead provides a comprehensive review of existing IDS techniques. It highlights the need for more robust and sophisticated methods to detect and mitigate cyber threats in SCADA systems, which are critical to national infrastructure. The paper suggests improvements in IDS for enhanced SCADA security, emphasizing the importance of adapting to evolving cyber threats.

7. Results

While most of the cloud security reviews presently available are dominantly focused on traditional security, a few have stretched to include machine learning applications. None of them gave an overview of the integration between machine learning and real-time threat intelligence. Our review closes this gap since it is an inclusive synthesis of these two areas; it underlines the combined potential to improve the security of cloud environments beyond the capabilities of stand-alone methods.

The findings from the analyzed research papers are summarized in Tables 1 and 2 below. These tables provide a comprehensive overview of the different approaches used by the papers, focus areas, and evaluation methods used in the field of cloud security.

Interestingly, while many studies report high accuracy rates, such as those by [59,63], which achieved 97% and 99% accuracy respectively in detecting insider threats, there are some gaps and trends that stand out. These papers highlight the effectiveness of advanced models like ensemble learning and Deep Belief Neural Networks (DBNs) that clearly shows that machine learning is making significant strides in this domain.

However, one surprising finding from this review is the limited use of unsupervised learning techniques, especially combined with dynamic threat intelligence. Despite the massive potential of these methods to detect unknown threats without the need for labeled data, most studies, such as [57] and [60], still rely heavily on supervised learning approaches like Support Vector Machines (SVMs) and autoencoders.

Another trend that emerged these years is the relatively sparse integration of cyber threat intelligence (CTI) with machine learning models. Although CTI is recognized as a critical component for enhancing cloud security, studies like [58] and [61] show that many current models don't fully utilize the power of real-time threat intelligence. This gap indicates that there is significant room for developing integrated solutions that dynamically update ML models with real-time threat data.

 doi:10.20944/preprints202410.0512.v1

Table 1. Summary of Research Papers on Cloud security (Part 1).

Authors	ML Algorithms	Focus Area	Frameworks & Approaches	Evaluation Metrics	Security Requirements
[57]	Transfer Learning	Anomaly Detection, Cloud Security	Transfer learning for detecting known and unknown attacks	Not specified	Adaptability, Real-time detection
[58]	Not specified	Cyber Threat Intelligence Mining	Gathering and converting real-time cyber threat information	Not specified	Scalability, Accuracy
[59]	Ensemble Learning	Insider Threats, Privilege Escalation	Machine learning-based system for detecting insider threats	Accuracy (97%)	Real-time detection, Accuracy
[60]	K-means, SVMs, Autoencoders	Anomaly Detection, Cloud Security	Machine learning for anomaly detection in cloud environments	Not specified	Efficiency, Scalability
[61]	Not specified	Cyber Threat Intelligence Quality	Methodology for enhancing CTI quality	Not specified	Quality of Information
[62]	Machine Learning Models	CTI Analysis and Visualization	Machine learning models for training on attack patterns	Accuracy (86%)	Usability, Scalability
[63]	Deep Belief Neural Network	Insider Threat Detection	DBN for identifying malicious activities by legitimate users	Accuracy (99%), F-score (98%)	Accuracy, Confidentiality
[64]	Not specified	Cyber Threat Intelligence Sharing	Hybrid cloud-based deployment model for CTI sharing	Not specified	Scalability, Privacy
[65]	IPCA, GSCSO, IHNN	Cyber Threat Detection	Security model combining IPCA, GSCSO, and IHNN	Improved detection accuracy and F1-scores	Efficiency, Accuracy
[66]	Not specified	IoT-enabled Maritime Transportation Systems	DLTIF for modeling and identifying cyber threats	Accuracy (up to 99%)	Scalability, Real-time detection

 doi:10.20944/preprints202410.0512.v1

Table 2. Summary of Research Papers on Cloud security (Part 2).

Authors	ML Algorithms	Focus Area	Frameworks & Approaches	Evaluation Metrics	Security Requirements
[67]	Data Fusion, Machine Learning Classifiers	DDoS Attack Detection	Data fusion applications alongside ML classifiers	Not specified	Real-time detection, Accuracy
[68]	Not specified	Cybersecurity Knowledge Integration	Integrating malware behavior data with CTI	Not specified	Integrity, Scalability
[69]	Machine Learning, Deep Learning	Cloud Security	Analysis of ML/DL techniques in cloud security	Not specified	Adaptability, Efficiency
[42]	Machine Learning Algorithms	Attack Detection in Cloud	Detection of DDoS and MitC attacks using ML algorithms	Accuracy (100%)	Real-time detection, Accuracy
[70]	Not specified	Cyber Threat Intelligence Framework	CTI framework for incident response in energy cloud platforms	Macro-F1, Micro-F1 metrics	Scalability, Efficiency
[71]	Behavior-based, Signature-based, Anomaly-based Models	Cyber Threat Intelligence (CTI)	Framework for CTI implementation in organizations	Not specified	Usability, Accuracy
[72]	Not specified	Cyber Threat Intelligence Frameworks	Review and critique of existing cybersecurity frameworks	Not specified	Adaptability, Scalability
[73]	Multi-modal Hierarchical Attention Model	Phishing Detection	MMHAM for detecting phishing using website content	Not specified	Usability, Accuracy
[74]	Intrusion Detection Systems (Review)	SCADA Security	Review of IDS techniques for SCADA security	Not specified	Reliability, Scalability

 doi:10.20944/preprints202410.0512.v1

7.1. Discussion

Our review represents a fresh outlook; it takes a holistic examination of how machine learning and dynamic threat intelligence can be combined to harden cloud security. While several reviews have been conducted with regard to these technologies separately, our work represents one of the very few studies that take a look at their combined potential. What we found was that this integrated approach amped up the known threat detection capability, allowed for adaptability in real time against new and evolving risks. This is a quantum step forward from traditional security measures that are often static and cannot keep pace with the rapidly changing landscape of cyber threats.

Another striking observation is the partial integration of the threat intelligence with ML models. Despite all the benefits of real-time threat intelligence, many studies do not fully use this resource in their ML frameworks. Our review hence identifies that more work needs to be done to create models that keep updating and adapt to new information about the threats for stronger defense against both known and unknown attacks.

Our findings indicate quite a number of points that call for further investigation; for example, the elaboration of standardized metrics for evaluation and more scalable solutions. Addressing these gaps will, therefore, take the field one step closer toward creating stronger cloud security frameworks, better equipped to face the challenge of complexity imposed on it by today's digital environment.

7.2. Conclusion

This review concludes with a new look at machine learning and dynamic threat intelligence as complementing solutions for cloud security. We have shown that their broad application provides a far more flexible and effective cyber threat detection and response than afforded by traditional security. By highlighting key gaps in the research so far, we have clearly shown the way for future studies.

We believe that this review will not only present understandings but also inspire new ideas and directions for research and practice. In the future, it is highly expected to create adaptive and resilient security frameworks that keep pace with the fast evolution of cyber threats. Building on our findings and recommendations, we have no doubt in believing that both researchers and practitioners may further contribute to a more secure and robust cloud environment.

Author Contributions: Conceptualization, R.T. and B.R.; methodology, B.R. and R.T.; formal analysis, R.T., B.K., and A.M.; investigation, R.T.; resources, B.K. and A.M.; writing—original draft preparation, R.T. and B.R.; writing—review and editing, B.K. and A.M.; supervision, B.R.; project administration, B.R.; funding acquisition, B.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Project MESTI No. 2-2282-1.

Data Availability Statement: The data supporting the findings of this study are derived from publicly available sources. Each dataset used has been cited with either a Uniform Resource Identifier (URI) or a Digital Object Identifier (DOI) within the paper, providing direct access to the original sources. These references can be accessed freely to verify the research findings and to facilitate further study. No additional repository is used, ensuring transparency through the direct availability of all referenced data.

Acknowledgments: The authors gratefully acknowledge the Ministry of Education, Science, Technology and Innovation, Kosovo for supporting this research.

Conflicts of Interest: The authors declare no conflicts of interest. The funder had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Montazerolghaem, A.; Yaghmaee, M.H.; Leon-Garcia, A. Green Cloud Multimedia Networking: NFV/SDN based Energy-efficient Resource Allocation. *IEEE Transactions on Green Communications and Networking* **2020**, *PP*, 1–1. doi:10.1109/TGCN.2020.2982821.
2. Pallathadka, H.; Sajja, G.S.; Phasinam, K.; Ritonga, M.; Naved, M.; Bansal, R.; Quiñonez-Choquecota, J. An investigation of various applications and related challenges in cloud computing. *Materials Today: Proceedings*

 doi:10.20944/preprints202410.0512.v1

2022, *51*, 2245–2248. International Conference on Advances in Materials Science, doi:https://doi.org/10.1016/j.matpr.2021.11.383.

3. CLOUDZERO. 101+ Cloud Computing Statistics That Will Blow Your Mind, 2023. Accessed on 10 September 2024.
4. Khoda Parast, F.; Sindhav, C.; Nikam, S.; Izadi Yekta, H.; Kent, K.B.; Hakak, S. Cloud computing security: A survey of service-based models. *Computers & Security* **2022**, *114*, 102580. doi:https://doi.org/10.1016/j.cose.2021.102580.
5. Joshi, A.; Raturi, A.; Kumar, S.; Dumka, A.; Singh, D. Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks. 2022, pp. 230–233. doi:10.1109/ICFIRTP56122.2022.10063186.
6. Samuel, J.; Jacob, M.; Roy, M.; M, S.; Joy, A. Intelligent Malware Detection System Based on Behavior Analysis in Cloud Computing Environment. 2023, pp. 109–113. doi:10.1109/ICCPCT58313.2023.10245065.
7. Nassif, A.; Abu Talib, M.; Nasir, Q.; Albadani, H.; Albab, F. Machine Learning for Cloud Security: A Systematic Review. *IEEE Access* **2021**, *PP*, 1–1. doi:10.1109/ACCESS.2021.3054129.
8. Ferrag, M.A.; Shu, L.; Friha, O.; Yang, X. Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. *IEEE/CAA Journal of Automatica Sinica* **2021**. doi:10.1109/JAS.2021.1004344.
9. Butt, U.; Mehmood, M.; Shah, S.B.; Amin, R.; Shaukat, M.; Raza, S.; Suh, D.; Piran, M. A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics* **2020**, *9*, 1379. doi:10.3390/electronics9091379.
10. De Santo, A.; Galli, A.; Gravina, M.; Moscato, V.; Sperlì, G. Deep Learning for HDD health assessment: an application based on LSTM. *IEEE Transactions on Computers* **2020**, *PP*, 1–1. doi:10.1109/TC.2020.3042053.
11. Team, A.R. 2024 Cybersecurity Trends: AI, Cloud, and Threat Intelligence, 2024. Accessed on 15 August 2024.
12. Gangwani, D.; Sanghvi, H.; Parmar, V.; Patel, R.; Pandya, A., A Comprehensive Review on Cloud Security Using Machine Learning Techniques; 2023; pp. 1–24. doi:10.1007/978-3-031-28581-3_1.
13. Chauhan, M.; Shiaeles, S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network* **2023**, *3*, 422–450. doi:10.3390/network3030018.
14. Shah, Y.; Sengupta, S. A survey on Classification of Cyber-attacks on IoT and IIoT devices. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020, pp. 0406–0413. doi:10.1109/UEMCON51285.2020.9298138.
15. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review* **2019**, *33*, 1–48. doi:https://doi.org/10.1016/j.cosrev.2019.05.002.
16. Zhao, T.; Lechner, U.; Pinto-Albuquerque, M.; Ata, E. Cloud of Assets and Threats: A Playful Method to Raise Awareness for Cloud Security in Industry. Third International Computer Programming Education Conference (ICPEC 2022), 2022, Vol. 102, *Open Access Series in Informatics (OASIcs)*, pp. 6:1–6:13. doi:10.4230/OASIcs.ICPEC.2022.6.
17. Yeh, T.; Chen, Y. Improving the hybrid cloud performance through disk activity-aware data access. *Simulation Modelling Practice and Theory* **2021**, *109*, 102296.
18. Razaque, A.; Li, Y.; Liu, Q.; Khan, M.J.; Doulat, A.; Almiani, M.; Alflahat, A. Enhanced risk minimization framework for cloud computing environment. 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2018, pp. 1–7.
19. IBM. What is private cloud?, 2024. Accessed on 17 September 2024.
20. Khan, M.J.; Ullah, F.; Imran, M.; Khan, J.; Khan, A.; AlGhamdi, A.S.; Alshamrani, S.S. Identifying Challenges for Clients in Adopting Sustainable Public Cloud Computing. *Sustainability* **2022**, *14*. doi:10.3390/su14169809.
21. Meng, S.; Luo, L.; Qiu, X.; Dai, Y. Service-oriented reliability modeling and autonomous optimization of reliability for public cloud computing systems. *IEEE Transactions on Reliability* **2022**, *71*, 527–538.
22. Cloud, G. What is a Hybrid Cloud?, 2024. Accessed on 10 September 2024.
23. Marcu, R.; Danila, I.; Popescu, D.; Chenaru, O.; Ichim, L. Message Queuing Model for a Healthcare Hybrid Cloud Computing Platform. *Studies in Informatics and Control* **2017**, *26*, 95–104. doi:10.24846/v26i1y201711.
24. Tutorialspoint. Community Cloud Model, 2024. Accessed on 18 September 2024.
25. Spiceworks. What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, 2024. Accessed on 17 September 2024.
26. Tabrizchi, H.; Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing* **2020**, *76*. doi:10.1007/s11227-020-03213-1.

27. CrowdStrike. CrowdStrike 2024 Global Threat Report, 2024. Accessed on 17 August 2024.
28. El Kafhali, S.; El Mir, I.; Hanini, M. Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering* **2022**, *29*, 223–246. doi:10.1007/s11831-021-09573-y.
29. Dewangan, R.R.; Soni, S.; Mishal, A. An Approach of Privacy Preservation and Data Security in Cloud Computing for Secured Data Sharing. *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)* **2024**.
30. Tan, C.B.; Hijazi, M.; Lim, Y.; Gani, A. A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends. *Journal of Network and Computer Applications* **2018**, *110*. doi:10.1016/j.jnca.2018.03.017.
31. Ong, Y.J.; Qiao, M.; Routray, R.; Raphael, R. Context-aware data loss prevention for cloud storage services. 2017 IEEE 10th International Conference on Cloud Computing (CLOUD). IEEE, 2017, pp. 399–406.
32. Statista. What are your biggest cloud security concerns?, 2021. Accessed on 27 August 2024.
33. Ananthoju, V.K.; Woldeyohanes, N.; Woinshet, Y.; Shah, A.; Kemal, M.; Ameha, D. A Novel Approach to Prevent Hijacking of Accounts in the Cloud. 2024.
34. Dawood, M.; Tu, S.; Xiao, C.; Alasmary, H.; Waqas, M.; Rehman, S.U. Cyberattacks and Security of Cloud Computing: A Complete Guideline. *Symmetry* **2023**, *15*. doi:10.3390/sym15111981.
35. Bisht, P.S.; Mishra, P.; Chauhan, P.; Joshi, R. HyperGuard: On designing out-VM malware analysis approach to detect intrusions from hypervisor in cloud environment. *International Journal of Grid and Utility Computing* **2023**, *14*, 356–367.
36. Win, S.; Thwin, M., Handling the Hypervisor Hijacking Attacks on Virtual Cloud Environment; 2019; pp. 25–50. doi:10.1007/978-3-030-30436-2_2.
37. Aldribi, A.; Traoré, I.; Moa, B.; Nwamuo, O. Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking. *Computers & Security* **2020**, *88*, 101646. doi:https://doi.org/10.1016/j.cose.2019.101646.
38. Bhardwaj, A.; Mangat, V.; Vig, R.; Halder, S.; Conti, M. Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. *Computer Science Review* **2021**, *39*, 100332. doi:https://doi.org/10.1016/j.cosrev.2020.100332.
39. Chowdhury, F.Z.; Kiah, L.B.M.; Ahsan, M.M.; Bin Idris, M.Y.I. Economic denial of sustainability (EDoS) mitigation approaches in cloud: Analysis and open challenges. 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 2017, pp. 206–211. doi:10.1109/ICECOS.2017.8167135.
40. Suaboot, J.; Fahad, A.; Tari, Z.; Grundy, J.; Mahmood, A.N.; Almalawi, A.; Zomaya, A.Y.; Drira, K. A Taxonomy of Supervised Learning for IDSs in SCADA Environments. *ACM Comput. Surv.* **2020**, *53*. doi:10.1145/3379499.
41. Kosek, A.M. Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model. 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), 2016, pp. 1–6. doi:10.1109/CPSRSG.2016.7684103.
42. Rexha, B.; Thaqi, R.; Mazrekaj, A.; Vishi, K. Guarding the Cloud: An Effective Detection of Cloud-Based Cyber Attacks using Machine Learning Algorithms. *International Journal of Online and Biomedical Engineering (iJOE)* **2023**, *19*, pp. 158–174. doi:10.3991/ijoe.v19i18.45483.
43. Sebastian, A.; Naseem, H.; Catal, C. Unsupervised Machine Learning Approaches for Test Suite Reduction. *Applied Artificial Intelligence* **2024**, *38*. doi:10.1080/08839514.2024.2322336.
44. P. Sherubha, S. P. Sasirekha, A.D.K.A.J.V.R.R.A.S.P.P.R.H.K. An Efficient Unsupervised Learning Approach for Detecting Anomaly in Cloud. *Computer Systems Science and Engineering* **2023**, *45*, 149–166. doi:10.32604/csse.2023.024424.
45. Sarhan, M.; Layeghy, S.; Moustafa, N.; Portmann, M. Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection. *Journal of Network and Systems Management* **2022**, *31*. doi:10.1007/s10922-022-09691-3.
46. Al-Mohannadi, H.; Awan, I.; Hamar, J. Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence. *Service Oriented Computing and Applications* **2020**, *14*. doi:10.1007/s11761-019-00285-7.

47. Kim, B.; Lowry, P. A Review and Theoretical Explanation of the 'Cyberthreat-Intelligence (CTI) Capability' that Needs to be Fostered in Information Security Practitioners and How this Can be Accomplished. *Computers & Security* **2020**, *92*, Article: 101761.
48. Doynikova, E.; Novikova, E.; Kotenko, I. Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. *Information* **2020**, *11*. doi:10.3390/info11030168.
49. Irshad, E.; Basit Siddiqui, A. Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal* **2023**, *24*, 43–59. doi:https://doi.org/10.1016/j.eij.2022.11.001.
50. Forbes. What Is Threat Intelligence? Definition, Types & Process, 2023. Accessed on 27 August 2024.
51. Nova, K. Security and resilience in sustainable smart cities through cyber threat intelligence. *International Journal of Information and Cybersecurity* **2022**, *6*, 21–42.
52. Samtani, S.; Abate, M.; Benjamin, V.; Li, W. Cybersecurity as an industry: A cyber threat intelligence perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance* **2020**, pp. 135–154.
53. Raddatz, M. Threat Modeling in Machine Learning **2022**. *2*, 173–179. doi:10.52825/ocp.v2i.161.
54. Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy* **2022**, *2*, 527–555. doi:10.3390/jcp2030027.
55. Aldallal, A.; Alisa, F. Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning. *Symmetry* **2021**, *13*. doi:10.3390/sym13122306.
56. Abbas, Z.; Myeong, S. Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment. *Electronics* **2023**, *12*. doi:10.3390/electronics12122650.
57. Sreelatha .., G.; Babu, A.; Midhunchakkaravarthy, D. Ensuring Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning. 2020, pp. 666–670. doi:10.1109/ICCES48766.2020.9138009.
58. Sun, N.; Ding, M.; Jiang, J.; Xu, W.; Mo, X.; Yonghang, T.; Zhang, J. Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials* **2023**, *PP*, 1–1. doi:10.1109/COMST.2023.3273282.
59. Mehmood, M.; Amin, R.; Muslam, M.; Xie, J.; Aldabbas, H. Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. *IEEE Access* **2023**, *PP*, 1–1. doi:10.1109/ACCESS.2023.3273895.
60. Yerasuri, S.S. Enhancing Security in Cloud Computing with Anomaly Detection Using Machine Learning. *Tuijin Jishu/Journal of Propulsion Technology* **2023**, *44*, 1923–1931. doi:10.52783/tjjpt.v44.i3.622.
61. Machado da Silva, R.; Costa Gondim, J.J.; de Oliveira Albuquerque, R. Methodology to Improve the Quality of Cyber Threat Intelligence Production Through Open Source Platforms. International Conference on Computer Science, Electronics and Industrial Engineering (CSEI). Springer, 2022, pp. 86–98.
62. Ejaz, S.; Noor, U.; Rashid, Z. Visualizing Interesting Patterns in Cyber Threat Intelligence Using Machine Learning Techniques. *Cybernetics and Information Technologies* **2022**, *22*, 96–113. doi:10.2478/cait-2022-0019.
63. Arasan, A.; Kannadasan, R.; Joseph, N.; Boominathan, P.; G R, S. Insider Attack Detection Using Deep Belief Neural Network in Cloud Computing. *Computer Systems Science and Engineering* **2021**, *41*, 479–492. doi:10.32604/csse.2022.019940.
64. Heo, J.; Gebremariam, Y.; Park, H.; Kim, B.; You, I. Study on Hybrid Cloud-based Cyber Threat Intelligence Sharing Model Requirements Analysis. 2020, pp. 1–6. doi:10.1145/3440943.3444737.
65. Ramachandran, D.; Albathan, M.; Hussain, A.; Abbas, Q. Enhancing Cloud-Based Security: A Novel Approach for Efficient Cyber-Threat Detection Using GSCSO-IHNN Model. *Systems* **2023**, *11*, 518. doi:10.3390/systems11100518.
66. Kumar, P.; Gupta, G.; Tripathi, R.; Garg, S.; Hassan, M. DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2021**, *PP*, 1–10. doi:10.1109/TITS.2021.3122368.
67. Pattnaik, L.; Swain, P.; Satpathy, S.; Panda, A. Cloud DDoS Attack Detection Model with Data Fusion & Machine Learning Classifiers. *ICST Transactions on Scalable Information Systems* **2023**. doi:10.4108/eetsis.3936.
68. Piplai, A.; Mittal, S.; Abdelsalam, M.; Gupta, M.; Joshi, A.; Finin, T. Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior. 2020, pp. 1–6. doi:10.1109/ISI49825.2020.9280512.
69. Belal, M.; Sundaram, D. Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends. *Journal of King Saud University - Computer and Information Sciences* **2022**, *34*. doi:10.1016/j.jksuci.2022.08.035.

70. Gong, S.; Lee, C. Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. *Electronics* **2021**, *10*, 239. doi:10.3390/electronics10030239.
71. Saeed, S.; Suayyid, S.; Al-Ghamdi, M.; Al-Muhaisen, H.; Almuhaideb, A. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors* **2023**, *23*, 7273. doi:10.3390/s23167273.
72. Irfan, A.; Chuprat, S.; Mahrin, M.; Ariffin, A. Taxonomy of Cyber Threat Intelligence Framework. 2022, pp. 1295–1300. doi:10.1109/ICTC55196.2022.9952616.
73. Chai, Y.; Yonghang, Z.; Li, W.; Jiang, Y. An Explainable Multi-Modal Hierarchical Attention Model for Developing Phishing Threat Intelligence. *IEEE Transactions on Dependable and Secure Computing* **2021**, *PP*, 1–1. doi:10.1109/TDSC.2021.3119323.
74. Qassim, Q.; Jamil, N.; Mahdi, M.; Abdul Rahim, A.A. Towards SCADA Threat Intelligence based on Intrusion Detection Systems - A Short Review. 2020, pp. 144–149. doi:10.1109/ICIMU49871.2020.9243337.