Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies

Sina Ahmadi

Scientific Research Publishing

Journal of Information Security, 2024, 15, 148-167
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies

Sina Ahmadi

National Coalition of Independent Scholars, Seattle, United States
Email: sina0@acm.org

How to cite this paper: Ahmadi, S. (2024) Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, **15**, 148-167.
https://doi.org/10.4236/jis.2024.152010

Received: February 20, 2024
Accepted: March 24, 2024
Published: March 27, 2024

Abstract

Cloud computing plays a significant role in modern information technology, providing organizations with numerous benefits, including flexibility, scalability, and cost-efficiency. However, it has become essential for organizations to ensure the security of their applications, data, and cloud-based networks to use cloud services effectively. This systematic literature review aims to determine the latest information regarding cloud computing security, with a specific emphasis on threats and mitigation strategies. Additionally, it highlights some common threats related to cloud computing security, such as distributed denial-of-service (DDoS) attacks, account hijacking, malware attacks, and data breaches. This research also explores some mitigation strategies, including security awareness training, vulnerability management, security information and event management (SIEM), identity and access management (IAM), and encryption techniques. It discusses emerging trends in cloud security, such as integrating artificial intelligence (AI) and machine learning (ML), serverless computing, and containerization, as well as the effectiveness of the shared responsibility model and its related challenges. The importance of user awareness and the impact of emerging technologies on cloud security have also been discussed in detail to mitigate security risks. A literature review of previous research and scholarly articles has also been conducted to provide insights regarding cloud computing security. It shows the need for continuous research and innovation to address emerging threats and maintain a security-conscious culture in the company.

Keywords

Cloud Security, Threat Analysis, Mitigation Strategies, Emerging Trends, Ethical Considerations, Data Analysis

1. Introduction

The utilization of cloud computing is increasing daily in information technology, providing organizations worldwide with cost-efficiency, scalability, and a high level of flexibility. When organizations integrate cloud computing into their network, it is essential to focus on cloud security, a collection of security measures specially designed to protect cloud-based infrastructure, data, and applications. These measures aim to ensure the authentication of devices and users, data privacy protection, and data and resource access control. With the shift of businesses towards cloud-based operations, the security of sensitive data becomes essential [1]. However, cloud computing presents inherent security challenges, which makes it necessary to understand effective mitigation strategies and potential threats. This systematic literature review aims to determine the current state of information regarding cloud computing security, which primarily focuses on identifying threats and evaluating mitigation strategies.

Cloud services have revolutionized how organizations store, process, and access data. However, this shift has created several challenges, such as unauthorized access and data breaches, which have an impact on data availability, integrity, and confidentiality. Organizations must understand these threats and acquire knowledge on how to develop defensive strategies in order to utilize a secure cloud network. This research reviews several scholarly articles and papers to provide a detailed overview of significant security threats in cloud computing. It also includes human-related risks and technical vulnerabilities and evaluates existing mitigation strategies. Thus, this systematic research contributes to a deeper understanding of cloud computing. The primary objective of this research study is to identify cloud security threats and evaluate the efficiency of different mitigation strategies employed by organizations to address these threats. This research study also aims to explore emerging trends like ML, AI, containerization, and serverless computing. It assesses shared responsibility models, ethical considerations, user awareness, cloud computing and data security as shown in **Figure 1**.

2. Literature Review

2.1. Common Threats to Cloud Computing Security

Cloud computing is susceptible to numerous prevalent threats. This is because it is an entirely technology-based platform, making it susceptible to potential cyber threats at any given moment. For instance, data breaches are prevalent in this case. They result in unauthorized access to data or data theft. Furthermore, data breaches expose an organization's private information, which results in adverse reputational and financial outcomes. A prior study [3] was conducted in this regard. According to the researchers, data breaches force companies to implement strict security measures to protect data. Malware attacks are also widespread in this regard. These attacks include using software that hacks the cloud server and steals all the desired data. Another study [4] researched the prediction of such

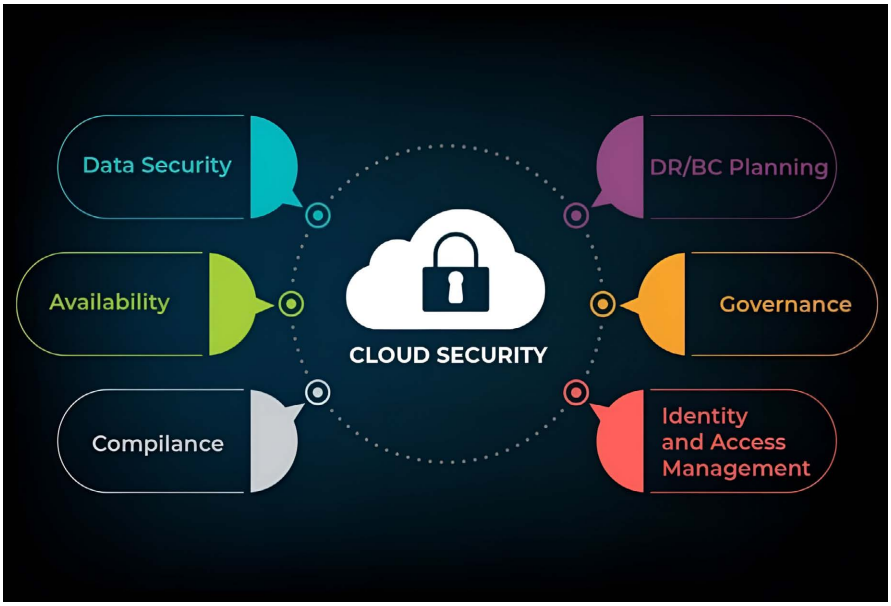

Figure 1. Cloud computing and data security [2].

attacks using machine learning. This is a great technique that tech companies can use to secure their data.

Account hijacking has also become a common practice in cloud computing. It is mainly used in identity theft schemes. In this case, the attacker uses a person's private information to conduct any other unauthorized or suspicious activity. Usually, compromised email accounts are used to impersonate a person. A prior study [5] on this issue proposed prevention strategies. In this case, it is important to encrypt data and private information. Lastly, DDoS attacks are also common in cloud computing. According to [6], these attacks aim to disrupt the regular working of a company's system by enhancing traffic on it. They can be very harmful to a company's reputation.

2.2. Mitigation Strategies in Cloud Security

Different mitigation strategies are used to ensure cloud security. However, the most common are the encryption techniques. Data encryption mainly ensures data conversion into an unreadable format, which can only be read with the help of the correct decryption keys. These encryption techniques have been utilized to secure data storage [7]. It was found that these techniques are highly effective in ensuring cloud security. The encryption benefits in a cloud network are described in **Figure 2**.

The effectiveness of encryption in preserving data integrity can be mathematically expressed by Equation (1) [3].

$$\text{Data Integrity} = \frac{\text{Number of Correctly Decrypted Messages}}{\text{Total Number of Encrypted Messages}} \times 100\% \quad (1)$$

IAM is another common technique used in this regard. According to [9], IAM controls access to services and resources inside the cloud environment based on

Figure 2. Encryption in a cloud network [8].

the least privilege principle. It allows only authorized users to access private data.

The efficiency of IAM strategies in controlling user access can be represented by Equation (2) [5].

$$\text{Access Control Efficiency} = \frac{\text{Number of Authorized Access Requests}}{\text{Total Number of Access Requests}} \times 100\% \quad (2)$$

Furthermore, SIEM solutions are used in cloud computing for data protection. According to [10], these solutions analyze the data of a security event using different sources in the cloud. By doing so, they help gain real-time information about the company's security situation. Another technique, according to Sasubuili and Venkateswarlu (2021), is vulnerability management. It mainly includes identifying and mitigating security vulnerabilities in a cloud environment. This measure significantly mitigates the risk of attacks.

The capability of SIEM solutions for early threat detection can be measured using the Formula (3) [7].

$$\text{Detection Rate} = \frac{\text{Number of Detected Threats}}{\text{Total Number of Threats}} \times 100\% \quad (3)$$

2.3. Emerging Trends in Cloud Security

Currently, many new trends are emerging in cloud security. One example of this is containerization. This technique includes developing and implementing software applications and their dependencies in portable containers that provide isolation and can be implemented quickly. According to [11], this method effectively ensures cloud security. By adopting this technology, organizations may face challenges regarding data governance and regulatory compliance. Thus, it is important to ensure that sensitive data within containers adhere to industry regulations such as HIPAA or DGPR.

Serverless computing is another emerging trend that is very effective. This method involves the development of an application model, which helps developers create and run application codes without using servers or backend infrastructure [12]. Some common examples include AWS Lambda, IBM, and Google

Cloud. Serverless computing offers numerous benefits but poses integration concerns, especially when integrating it with existing on-premises systems or third-party services. It is important to ensure seamless communication between serverless functions and other components of the application architecture for maintaining security and performance.

Artificial intelligence and ML are also increasingly being utilized to ensure cloud security. These techniques involve automated systems that help detect and mitigate cloud threats. The effectiveness of these techniques in cloud computing has been studied [13]. It was found that these methods greatly enhance the performance of cloud servers and ensure high levels of security. They also help enhance threat detection and mitigation; however, their implementation imposes challenges regarding model transparency and data privacy. Thus, organizations must explore regulatory requirements such as data protection laws and address ethical considerations related to the usage of AI algorithms for security purposes.

Quantum computing (QC) is another technique being used today. Cloud users can access different quantum resources online and perform quantum algorithms without specialized hardware. According to [14], QC can revolutionize tech firms in the future. Quantum computing aims to solve complex computational problems; however, its integration into cloud infrastructures raises concerns about cryptographic vulnerabilities. To address this issue, organizations must address the need for quantum-resistant encryption algorithms to protect sensitive data in the cloud.

2.4. Impact of Emerging Technologies on Cloud Security

Emerging technologies are currently revolutionizing cloud security. For instance, the use of serverless computing and containerization has highly improved the performance of cloud servers. They mainly enhance the agility and scalability of cloud servers. According to [15], companies must use various mitigation strategies and best practices to overcome the security challenges of diverse emerging technologies. Regular vulnerability scans are fundamental in this case since they can help assess a company's security level.

The use of ML and AI also needs proper mitigation strategies. For instance, the ML models used in the cloud need to be updated constantly. The outdated models being used in a company can lead to security attacks. According to [16], companies must use alternative but safe techniques. For instance, quantum-resistant cryptographic algorithms can be used in the cloud to reduce the risk of attacks. However, conducting regular risk assessments is the most critical step for all companies to ensure high levels of cloud security.

2.5. Quantitative Analysis of Threats and Mitigation Strategies

Using statistical methods and mathematical models facilitates the quantitative analysis of existing cloud security mitigation strategies. For example, probabilistic risk assessment (PRA) is a suitable technique in this case. According to [17],

PRA can help evaluate the effectiveness of the methods used in identifying and mitigating cloud security threats. It is a quantitative technique that calculates the likelihood of security issues. Another example is an e-commerce company migrating its customer database to the cloud. In this case, PRA reveals that the likelihood of a data breach due to insecure API endpoints is 70%. The organizations can allocate resources to strengthen API security measures by determining the probability of this specific threat. Bayesian networks are also employed for this purpose. They include graphical models that show the dependencies between different variables within the cloud. Several studies [18] also investigated the utilization of these networks for risk assessment. It was found that they can help show the complicated links between threats and the employed mitigation strategies. For example, a software development company using cloud infrastructure for code repositories employs Bayesian networks to model dependencies between software vulnerabilities and deployment configurations. By accurately predicting 80% of security incidents, the organization identifies critical vulnerabilities early in the development lifecycle, reducing the risk of exploitation in production environments.

Queuing theory is another important model that can be used to analyze mitigation strategies. This theory is used to understand the behavior of cloud resources under various workload conditions. This helps in assessing their performance in response to security threats. For example, a queuing theory model was developed to study the effectiveness of cloud applications in the healthcare industry [19]. It was found that the queuing theory helps a company improve its resource allocation processes and capacity planning to overcome the impact of security threats. Currently, game theory is being used to assess cloud security measures. This theory helps in understanding the links between defenders and attackers within the cloud. According to [20], this theory can be used by companies to create efficient defense mechanisms and improve their cloud security measures. The utilization of mathematical models greatly enhances the effectiveness of cloud security measures.

Table 1 shows the mathematical models that help quantitatively analyze current mitigation strategies used in cloud security.

Table 1. Mathematical models in cloud security.

Mathematical Model	Description	Formula	Example
Probabilistic Risk Assessment (PRA)	Evaluates the effectiveness of identifying and mitigating security threats	$\frac{\text{Number of Identified Threats}}{\text{Total Number of Threats}} \times 100\%$	PRA Score = (25/30) * 10 = 8.3
Queuing Theory Analysis	Analyzes cloud resource behavior under workload conditions	$\frac{\text{Number of Improved Processes}}{\text{Total Number of Processes}} \times 100\%$	Queuing Theory Effectiveness = (9/10) * 10 = 9.0
Bayesian Network Analysis	Identifies dependencies between variables in cloud environments	$\frac{\text{Number of Accurate Predictions}}{\text{Total Number of Predictions}} \times 100\%$	Bayesian Network Score = (35/40) * 10 = 8.75

3. Problem Definition

In this digital world, cloud computing is gaining increasing adoption as it offers scalability and flexibility for organizations. This transition has provided several benefits and security challenges, necessitating the protection of the cloud storage system. Several solutions are already available to deal with such security threats, such as the shared responsibility model and emerging technologies, to promptly mitigate risks associated with human errors. However, it is imperative to prioritize advanced threats and employ mitigation strategies to adequately protect and preserve the cloud system.

This research investigates the evolving landscape of cloud security by emphasizing key challenges, such as the dynamic threat environment and complexities within the shared responsibility paradigm. The study aims to contribute to existing literature by focusing on these issues, informing strategies for mitigating cloud security risks and developing a more resilient security posture in cloud-based environments.

3.1. Evolving Threat Landscape

One of the significant challenges regarding cloud system security is the complex and constantly changing nature of cyber threats [21]. The attackers focus on developing new strategies and methods to hack an organization's data, which can harm the organization. Thus, a robust security system is essential to dealing with evolving threats in the industry. For instance, when a new threat is introduced or emerges, it becomes difficult for a traditional security solution to protect an organization's data, which makes the cloud environment open to sophisticated attacks. As a result, developing an adaptive security approach that can deal with cyber threats is necessary.

3.2. Shared Responsibility Model Challenges

The shared responsibility model is one of the most common models used in cloud computing; however, this model has resulted in several challenges between clients and cloud service providers [22]. Cloud providers are responsible for the security of the infrastructure, while clients play an essential role in securing their applications and data. This division of responsibilities can create security gaps and confusion. When these responsibilities are misunderstood, it may result in oversight, misconfiguration, or neglect of essential security measures. In addition, when organizations use the shared responsibility model, it demands communication, clarity, and a shared commitment toward strong security practices from both ends.

3.3. Impact of Emerging Technologies

Advanced technologies play an essential role in every field of life, regardless of industry. The two most important emerging technologies in cloud computing are serverless computing and containerization [23]. These technologies have

played an essential role in changing how applications are developed and deployed in cloud environments. In addition, these technologies come with a high level of agility, making them helpful for organizations to deal with security challenges. For instance, containers are significant in bridging the risk of vulnerabilities and misconfigurations, which attackers may exploit. Moreover, serverless computing raises concerns regarding the secure processing and storage of data. Thus, there is a great need to understand the risks and characteristics of emerging technologies if traditional security measures are being adopted.

3.4. Lack of User Awareness and Human Error

One of the primary reasons for conducting this research is to enhance user awareness and reduce human error. Human errors are among the most common reasons for security breaches in cloud-based environments [24]. Cloud computing is enriched with technical measures but may include issues like weak passwords, misconfigurations, and the leakage of sensitive information. These issues may occur due to insufficient user awareness. Moreover, organizations need help in educating users regarding security practices and fostering a culture that prioritizes security. For this purpose, focusing on effective security awareness programs to mitigate human-related cyber threats is essential. This study emphasizes the importance of communication with the users and their continuous training to develop a sense of responsibility among them.

To overcome this issue, organizations need to implement interactive e-learning courses, simulated phishing exercises, and gamified learning experiences to educate users on security best practices. They must regularly communicate security updates through email newsletters, intranet announcements, and in-person workshops to keep users informed. In addition, they should gain leadership support for security initiatives and incentivize security-conscious behavior through rewards programs and performance evaluations.

4. Methodology/Approach

4.1. Research Design

This study used a qualitative research design to analyze and synthesize existing studies, such as research papers and scholarly articles on cloud computing security. The qualitative research method explored the nature of cloud security threats and mitigation strategies. This approach involved carefully selecting scholarly articles and other research studies published between 2020 and 2024. The objective was to identify several significant threats and evaluate mitigation strategies. Additionally, this approach provides insights regarding the effectiveness and limitations of existing security measures in cloud-based networks. This study utilized a qualitative research design to analyze existing studies on cloud computing security. While qualitative research offers valuable insights into the nature of threats and mitigation strategies, it is subject to biases inherent in the interpretation of data.

4.2. Biases and Limitations

As with any qualitative approach, there are potential biases and limitations to consider. The interpretation of findings may be influenced by researchers' subjective perspectives, which leads to possible researcher bias. Additionally, the selected research papers and scholarly articles may not explain cloud security issues in detail, which introduces potential sampling bias.

4.3. Research Setting and Participants

Google Scholar was utilized as the setting for this study, from which past research studies were selected. This platform offers users access to scholarly articles, books, and research papers on top cloud computing security. The participants in this research study include the researchers and authors who have contributed to the literature review section. By selecting all the relevant research studies based on specific themes, this research aims to focus on threats and mitigation strategies highlighted in the period from 2020 to 2024. The time period was limited because the field of cloud computing has ever-changing trends. That's why it was important for the study to consider only the recent trends in cloud computing security.

4.4. Data Collection

The data collection for this research study included a structured approach for identifying valuable and relevant research papers and scholarly articles on cloud computing security. First, a thorough examination of Google Scholar was conducted by applying a year filter, specifically setting the range from 2020 to 2024. Subsequently, a specific theme related to this research study was queried in the Google Scholar search field. The most relevant research papers that included all or most keywords, such as cloud computing threats, security, and mitigation strategies, were selected. While efforts were made to systematically identify and select relevant research papers, the search criteria and selection process may have inadvertently excluded certain studies. This could introduce selection bias and impact the comprehensiveness of the literature review.

4.5. Inclusion and Exclusion Criteria

The inclusion criteria for this research study encompassed research papers, books, and research papers published between 2020 and 2024. The primary focus of these research studies was on cloud computing security to address different topics, such as mitigation strategies, threats, and vulnerabilities. All the selected papers were written in English, including the analysis and synthesis of data related to cloud computing security. The exclusion criteria encompassed studies published before 2019 and those without any of the keywords pertinent to this research study, *i.e.*, cloud security issues.

4.6. Data Analysis

Data analysis for this research study involved utilizing a thematic approach

based on which the literature review was conducted. The purpose of creating themes was to extract meaningful patterns and insights from the selected research studies. First, the literature was organized into relevant themes based on the topics identified in the data—the thematic analysis aimed to identify emerging trends in cloud computing security and threats and mitigation strategies. Subsequently, the findings of all the research studies were summarized and synthesized to extract useful and up-to-date information that could provide insights into cloud security.

4.7. Ethical Considerations

In this systematic literature review, ethical considerations are integral to ensuring the confidentiality and integrity of the data collected and analyzed. Necessary measures were taken to follow ethical standards and guidelines throughout the research process. Proper citation practices and intellectual property rights were also considered when the included research studies were cited. Original authors and researchers were also credited for their original work through referencing. In addition, the confidentiality of individuals' data was maintained, as no primary data was involved in this research study that involved the participants' data. Similarly, honesty and transparency were prioritized when reporting as a prop, and all the consulted sources were given attribution. The purpose of addressing ethical considerations is to follow the principles of research ethics and academic integrity. Ethical considerations were integral to maintaining the integrity of the research process. However, it is important to acknowledge that biases, both conscious and unconscious, may influence data interpretation and reporting despite adherence to ethical guidelines. Therefore, transparency and reflexivity in reporting findings are crucial for mitigating potential biases.

5. Results and Discussion

5.1. Unveiling Common Threats

The common threats in cloud security include some challenges organizations face in directing their data [25]. Data breaches, characterized by unauthorized access to sensitive data, are a common challenge. These breaches compromise some critical data, creating a significant risk for organizations. Malware attacks also present concerns with dangerous software that aims to disturb operations or affect data integrity. This malware exploits vulnerabilities in cloud systems, emphasizing the need to create robust security measures to detect and prevent this cyber infection. Account hijacking, in which the unauthorized user gains control over data, emphasizes the risk of unauthorized access to sensitive data and its misuse. In addition, DDoS threats disturb services by overpowering the system with a large amount of traffic, which highlights the importance of adequate security measures to confirm the safety of cloud services. Solving these challenges is essential for organizations to enhance the security and integrity of their cloud systems. In this evolving cloud security system, organizations must remain pre-

pared for imminent threats. Data breaches, account hijacking, and DDoS threats collectively show a dynamic challenge that requires the adoption of solid security measures. Understanding these challenges becomes essential to developing countermeasures as cloud technology advances. Thus, through a thorough analysis of these threats, organizations can design their security measures to decrease the risks, which ensures a reliable and secure cloud system. Some common cloud security threats are shown in Figure 3.

5.2. Vulnerability Spotlight: Data Breaches

Data breaches present a severe challenge with significant implications in the spotlight of weaknesses within cloud security [27]. Unauthorized access to sensitive data is included in data breaches, posing a risk for organizations and clients. The effect of data breaches stretches beyond the compromise of confidentiality, as they can lead the organization to financial losses, reputational damage, and other negative impacts. An attacker's unauthorized access to personal data, such as passwords or financial details, highlights the need for the implementation of solid security measures in cloud systems.

Essential protection plays an important role in securing cloud systems to mitigate the impact of data breaches. Encryption is also crucial in protecting sensitive data by converting it into an unreadable form, which makes it unintelligible

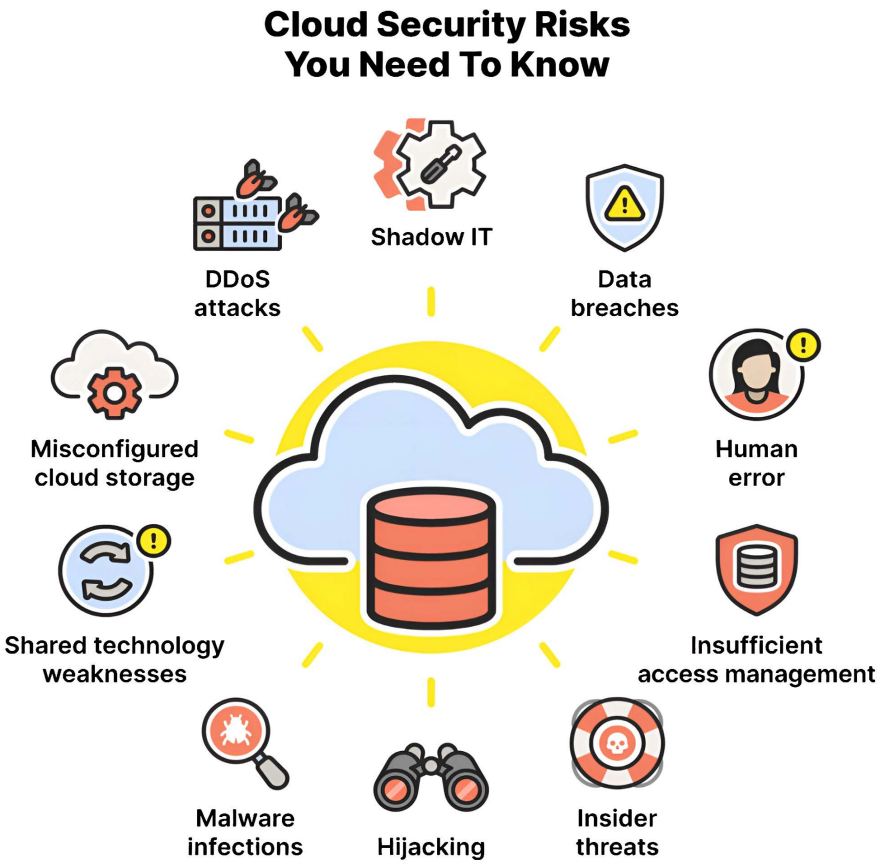

Figure 3. Common cloud security threats [26].

to unauthorized users. This security measure confirms that in the event an unauthorized user gains access, they will be unable to read the sensitive information. In addition, given these existing vulnerabilities, effective management is equally essential. It involves a systematic approach to identifying and solving the substantial flaws in the cloud system prior to their exploitation by hackers. This strategy involves regular security checks, removing weaknesses, and staying informed of imminent threats. By prioritizing these crucial protections, organizations can enhance their reliability against the effects of data breaches and create a more secure cloud system.

5.3. The Pervasiveness of Malware: SIEM Solutions

Malware attacks are the biggest problem for cloud security. Malware is harmful software that gets into cloud systems to cause damage [28]. These attacks occur due to software vulnerabilities. They are a significant concern due to their frequent occurrence and potential to result in serious consequences, such as the loss of sensitive data. To deal with malware attacks, it is essential to possess a comprehensive understanding of their nature and employ effective countermeasures. One crucial way to stay safe from malware is by using SIEM solutions. Security Information and Event Management assists in the surveillance of cloud activities and identifies any anomalous occurrences that may pose a security risk. By using SIEM, organizations can better protect themselves from malware attacks in the cloud [29].

5.4. IAM Empowerment: Account Hijacking

Exposing the challenges related to account hijacking is essential to understanding cloud systems' weaknesses. Account hijacking consists of unauthorized access to personal user accounts, which can lead to solid data misuse and illegal activities. This type of cyberattack generally utilizes weak passwords, phishing attacks, or other methods to gain control over users' data. The results of account hijacking can range from data breaches to unauthorized data access, making it essential for the organization to solve these challenges. Identity and access management is vital in mitigating the risk associated with account hijacking. It gives power to organizations to manage user authority over the data in the cloud system. By applying strong IAM practices, organizations can implement vital authentication steps such as multi-factor authentication and regularly update access permissions depending on user roles. Furthermore, IAM allows organizations to manage user activities, which enables the early detection of unauthorized access. Thus, IAM strategies are essential in maintaining cloud security by reducing the challenges related to account hijacking and confirming that only authorized users can access sensitive data.

5.5. Mitigation Strategies for DDoS Disruptions

Reducing DDoS attacks is essential to keeping cloud services stable, organized,

and available [30]. These attacks send traffic to the system and block actual users. Organizations use strategies, such as traffic filtering and irregularity detection, to deal with these situations. They also create a scalable structure and use content delivery networks to spread traffic. Some organizations apply specialized DDoS protection services. Monitoring traffic on the network can help organizations detect and address attacks early. It is also essential to have a plan for when attacks happen. Thus, by applying this step, organizations can reduce DDoS attacks, which keeps their services running smoothly for every user. Traffic filtering is also vital to dealing with DDoS attacks. It functions by stopping bad traffic and allowing good traffic to proceed. Organizations use tools like firewalls and intrusion prevention systems to check upcoming data. The main advantage of this tool is that it prevents lousy traffic from flooding the network. Load balancing also plays a vital role in this situation. It distributes traffic across multiple servers, thereby preventing server congestion and downtime. This ensures the continuity of services even during the attacks. Using these strategies, any organization can handle DDoS attacks more professionally. It ensures that their cloud services run smoothly without any disturbance in the network. Thus, any organization can stay protected from DDoS attacks by filtering the traffic and balancing the load. **Figure 4** shows DDoS mitigation strategies.

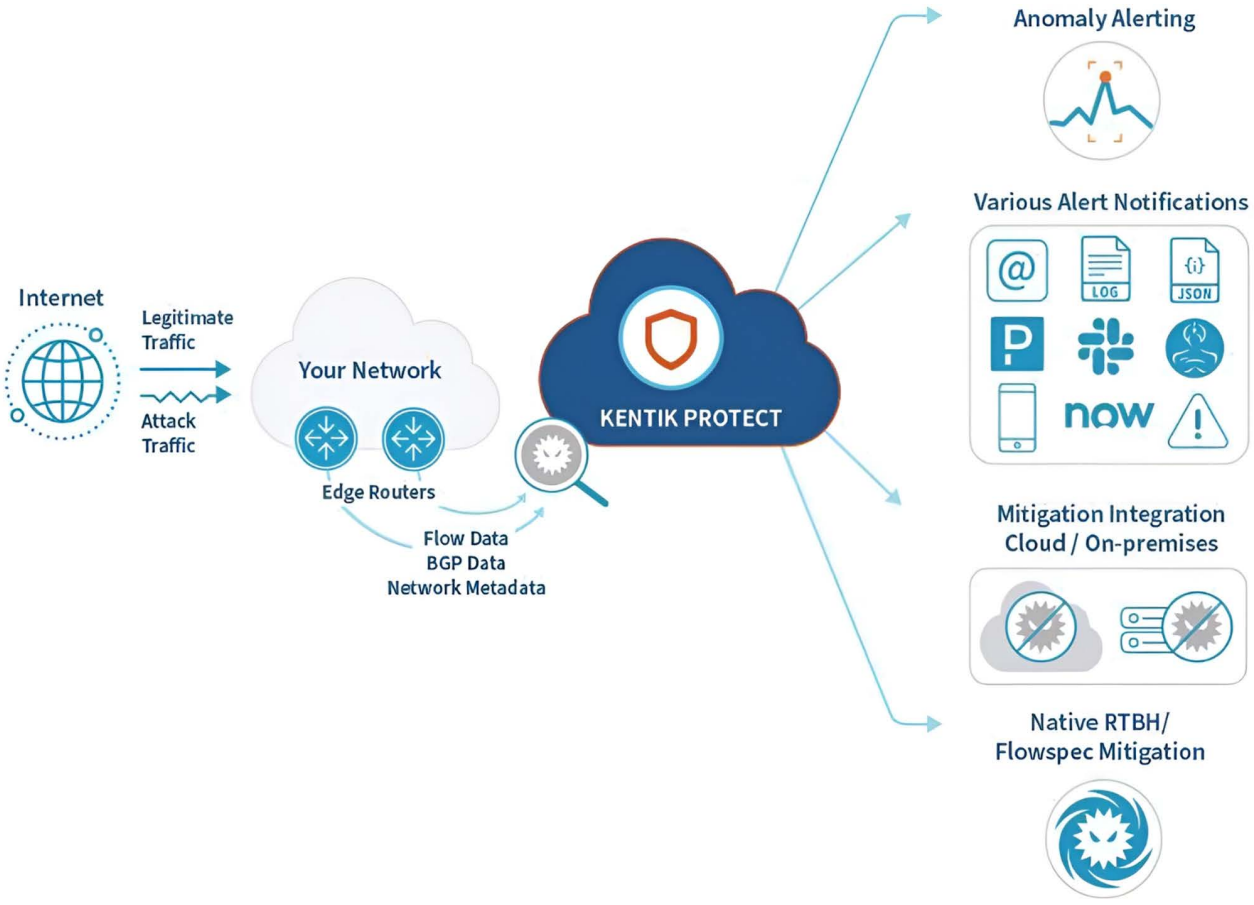

Figure 4. Mitigating DDoS disruptions [31].

5.6. Mitigating Threats: Defense Strategies

Reducing threats in cloud computing requires many defense strategies against attacks. At this rate, encryption is essential to protect sensitive data. Its main advantage is that it converts all data into unreadable code, which prevents any unauthorized access to the data. It is essential to maintain confidentiality and protect data from data breaches. Identity and access management is necessary for managing and monitoring user access to the data. The IAM solution contains strong authentication and manages user permissions based on their actions and roles, which protects data from unauthorized access and boosts security by limiting access to the necessary data. Security information and event management solutions are essential to detecting the attack early. They collect and analyze the data they fetch from different resources in the cloud environment, resulting in a smooth response and action to the strong attacks.

These solutions help organizations monitor security events in one frame, facilitating rapid detection. Vulnerability management helps find and fix a system's weaknesses through regular monitoring and checks. Security education is also essential to stay protected from attacks. All these defenses make a robust system for handling threats and accelerating cloud security. Thus, organizations can detect issues early by taking a central view of security events.

The effectiveness of vulnerability management in reducing potential weaknesses can be expressed through Equation (4) [27].

$$\text{Vulnerability Reduction} = \frac{\text{Initial Number of Vulnerabilities} - \text{Final Number of Vulnerabilities}}{\text{Initial Number of Vulnerabilities}} \quad (4)$$

5.7. Secure User Access: IAM Essentials

Ensuring secure user access to resources is crucial for maintaining and protecting the cloud environment. This goal is achieved with the help of IAM [32], a gatekeeper responsible for regulating and overseeing authorization and user authentication. According to this model, only authorized users are granted access to specific resources based on the tasks they need to perform in an organization. These users are provided with different permissions and roles to grant access based on each individual's job responsibilities, hence minimizing needless access.

Identity and Access Management is not limited to managing user access; it can also help organizations evaluate the activities of all users. This feature is helpful for organizations to monitor and audit the interaction of each user with cloud resources. Moreover, this real-time visibility enhances the ability to quickly find suspicious or unusual behavior. Additionally, IAM simplifies the overall process of managing user access rights and identities, strengthening the general security of the cloud environment. Therefore, integrating IAM into an organization ensures users have the appropriate access to perform their tasks effectively.

5.8. Integration of SIEM for Early Detection

Organizations need to develop an effective cloud computing security system for the early detection of threats and errors. They can use SIEM to detect early threats and ensure overall cloud security [33]. Security information and event management is like a guardian responsible for continuously collecting and analyzing data from different sources within the cloud network. This data may include activities, events, and logs generated by the applications, users, and infrastructure components. Security information and event management can also identify deviations, anomalies, or patterns from normal behavior, which may indicate the presence of a security threat. This mechanism of detecting errors early allows organizations to deal with security incidents effectively to minimize the impact of cyber threats.

Implementing SIEMs' early detection has a significant impact as it provides a basis for monitoring and managing security events. This system also enables the security teams to correlate important information and get insights regarding emerging threats. When this information is provided to security teams, it becomes easy for them to make valuable and appropriate decisions and focus on implementing effective responses and strategies. In addition, when the threats are detected early with the help of SIEM, it enhances an organization's ability to deal with cyber threats before facing significant issues related to data systems and business operations. Thus, SIEM is a defensive mechanism that allows organizations to secure sensitive data and business operations in the context of cloud security.

Figure 5 depicts the integration of SIEM for early detection of threats.

5.9. Awareness Training Programs for Users

Whenever a new technology or system is introduced, it is essential to educate the users to understand the purpose and usage of that technology or device. Similarly, when a security system is implemented in a cloud computing network to deal with potential threats, it is essential to provide detailed information to the users regarding that system to mitigate the risks associated with significant errors. Human errors are integral to security incidents within cloud networks as technology evolves [31]. Security awareness training programs aim to educate users about the importance of security policies, safe online practices, and potential threats. When a sense of responsibility is developed among users, it reduces the chances of data breaches and compromises the overall security of the cloud network.

The benefit of security awareness training programs also includes establishing a security-conscious environment where employees are informed about cybersecurity best practices as well as threats and mitigation strategies. This enables them to actively contribute to protecting sensitive resources and information within the organization. A security-conscious culture of an organization is characterized by a collective recognition of the importance of cybersecurity measures, fostering an environment where all employees are encouraged to report

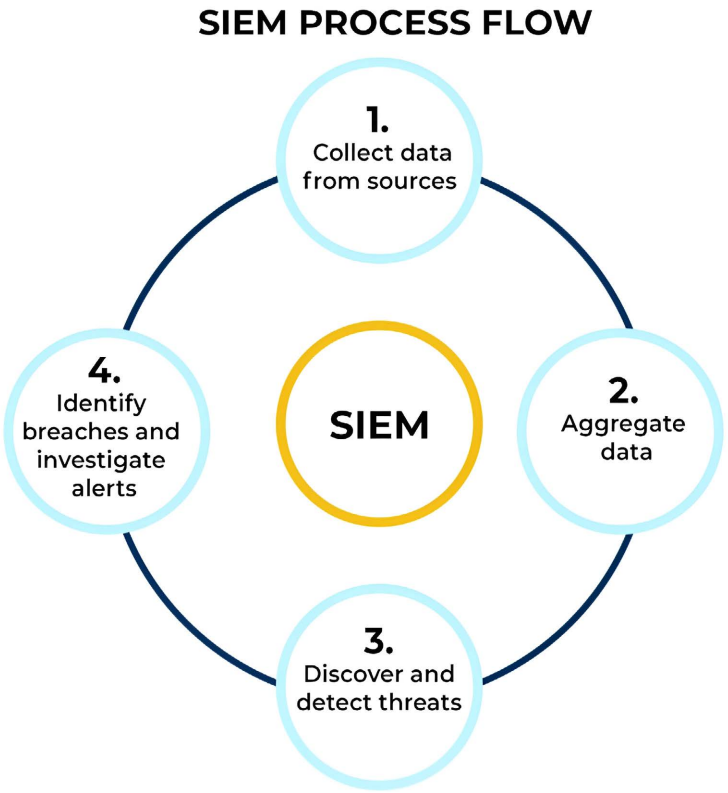

Figure 5. Integration of SIEM for early detection [34].

suspicious activities [33]. This culture follows security protocols and is integral to maintaining a secure cloud network. Thus, such training programs are not only for enhancing the knowledge of individuals but also to develop a sense of shared commitment to cybersecurity and help the organization deal with potential security threats.

The impact of security awareness training on reducing human errors can be quantified using formula (5) [31].

$$\text{Error Reduction} = \frac{\text{Initial Number of Security} - \text{related Errors} - \text{Final Number of Errors}}{\text{Initial Number of Security} - \text{related Errors}} \times 100\% \quad (5)$$

6. Conclusion

This systematic literature review evaluation on cloud computing security aims to determine adequate security measures to mitigate evolving threats quickly. The qualitative analysis highlights critical threats, including malware attacks and data breaches, emphasizing the need for encryption techniques, user awareness training, SIEM, and IAM. Some emerging trends in cloud computing security, such as AI and containerization, are also mentioned in this research. Moreover, ethical considerations and the shared responsibility model are essential in ensuring adequate security measures. The findings from the literature review guide effective cloud security practices. In addition, this research highlights areas that future researchers should consider to protect the confidentiality and integrity of

cloud-based systems.

7. Future Scope

The future scope of research in cloud computing security presents an exciting landscape filled with opportunities to address emerging challenges and advance the effectiveness of mitigation strategies. As technology evolves, several critical avenues merit exploration for researchers and practitioners. First, the advent of quantum computing introduces a novel dimension to cloud security. Researchers can delve into developing encryption methods specifically designed to withstand the computational capabilities of quantum machines. Understanding and mitigating the potential threats posed by quantum computing will be crucial to ensuring the long-term security of cloud environments. The proliferation of hybrid and multi-cloud architectures calls for focused attention in future research. Investigating security solutions that seamlessly integrate across diverse cloud platforms can enhance the overall resilience of organizations. Addressing the unique challenges of maintaining consistent security measures in hybrid and multi-cloud setups will ensure robust protection against evolving threats.

Given the increasing popularity of AI and ML applications, their role in enhancing cloud security deserves exploration. Future research could focus on refining AI/ML algorithms to bolster threat detection capabilities and provide more adaptive and responsive security solutions. Understanding the synergy between AI/ML and traditional security measures will be essential in developing comprehensive defense mechanisms. Additionally, the human element remains a critical factor in cloud security, and future research should emphasize strategies to fortify this aspect further. Developing innovative approaches to enhance user awareness and education programs can minimize the risk of human error and foster a security-conscious culture within organizations. Furthermore, the regulatory landscape governing cloud security is evolving. Future research could delve into the implications of emerging regulations and standards, ensuring that security practices align with compliance requirements. This includes examining how regulatory frameworks influence security policies and practices within cloud environments.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Vinoth, S., Vemula, H.L., Haralayya, B., Mamgain, P., Hasan, M.F. and Naved, M. (2022) Application of Cloud Computing in Banking and e-Commerce and Related Security Threats. *Materials Today*: *Proceedings*, **51**, 2172-2175. https://doi.org/10.1016/j.matpr.2021.11.121

[2] Kurt, E. (2022) Cloud Computing and Data Security. https://ekremkurt1907.medium.com/cloud-computing-and-data-security-cdce9745

ab09

[3] Chen, D., Chowdhury, M.M. and Latif, S. (2021) Data Breaches in Corporate Setting. 2021 *International Conference on Electrical*, *Computer*, *Communications and Mechatronics Engineering* (*ICECCME*), Mauritius, 7-8 October 2021, 1-6. https://doi.org/10.1109/ICECCME52200.2021.9590974

[4] Patel, V., Choe, S. and Halabi, T. (2020) Predicting Future Malware Attacks on Cloud Systems Using Machine Learning. *IEEE 6th International Conference on Big Data Security on Cloud*, Baltimore, 25-27 May 2020, 151-156. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00036

[5] Lokuge, K. (2020) Security Concerns in Cloud Computing: A Review. https://www.researchgate.net/publication/346606684_Security_Concerns_in_Cloud_Computing_A_Review

[6] Srinivasan, K., Mubarakali, A., Alqahtani, A.S. and Dinesh Kumar, A. (2020) A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In: Balaji, S., Rocha, Á. and Chung, Y.-N., Eds., *Intelligent Communication Technologies and Virtual Mobile Networks*, Springer, Berlin, 252-270. https://doi.org/10.1007/978-3-030-28364-3_24

[7] Seth, B., Dalal, S., Jaglan, V., Le, D.N., Mohan, S. and Srivastava, G. (2022) Integrating Encryption Techniques for Secure Data Storage in the Cloud. *Transactions on Emerging Telecommunications Technologies*, **33**, e4108.

[8] Ashtari, H. (2021) What Is Cloud Encryption? Definition, Importance, Methods, and Best Practices. https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-encryption/

[9] Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J. and Oladoyinbo, T.O. (2024) AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems. *Asian Journal of Research in Computer Science*, **17**, 38-56. https://doi.org/10.9734/ajrcos/2024/v17i3423

[10] Sasubilli, M.K. and Venkateswarlu, R. (2021) Cloud Computing Security Challenges, Threats and Vulnerabilities. 6*th International Conference on Inventive Computation Technologies*, Coimbatore, 20-22 January 2021, 476-480. https://doi.org/10.1109/ICICT50816.2021.9358709

[11] Bentaleb, O., Belloum, A.S., Sebaa, A. and El-Maouhab, A. (2022) Containerization Technologies: Taxonomies, Applications and Challenges. *The Journal of Supercomputing*, **78**, 1144-1181. https://doi.org/10.1007/s11227-021-03914-1

[12] Kelly, D., Glavin, F. and Barrett, E. (2020) Serverless Computing: Behind the Scenes of Major Platforms. *IEEE 13th International Conference on Cloud Computing* (*CLOUD*), Beijing, 19-23 October 2020, 304-312. https://doi.org/10.1109/CLOUD49709.2020.00050

[13] Rath, M., Satpathy, J. and Oreku, G.S. (2021) Artificial Intelligence and Machine Learning Applications in Cloud Computing and Internet of Things. In: Kaur, G., Tomar, P. and Tanque, M., Eds., *Artificial Intelligence to Solve Pervasive Internet of Things Issues*, Elsevier, Amsterdam, 103-123. https://doi.org/10.1016/B978-0-12-818576-6.00006-X

[14] Abidin, S., Swami, A., Ramirez-Asís, E., Alvarado-Tolentino, J., Maurya, R.K. and Hussain, N. (2022) Quantum Cryptography Technique: A Way to Improve Security Challenges in Mobile Cloud Computing (MCC). *Materials Today*: *Proceedings*, **51**, 508-514. https://doi.org/10.1016/j.matpr.2021.05.593

[15] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. and Ayaz, M. (2021)

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, **9**, 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

[16] Yau-Yeung, D., Yigitbasioglu, O. and Green, P. (2020) Cloud Accounting Risks and Mitigation Strategies: Evidence from Australia. *Accounting Forum*, **44**, 421-446. https://doi.org/10.1080/01559982.2020.1783047

[17] Gupta, I., Gupta, R., Singh, A.K. and Buyya, R. (2020) MLPAM: A Machine Learning and Probabilistic Analysis Based Model for Preserving Security and Privacy in Cloud Environment. *IEEE Systems Journal*, **15**, 4248-4259. https://doi.org/10.1109/JSYST.2020.3035666

[18] Chen, C., Zhang, L. and Tiong, R.L.K. (2020) A Novel Learning Cloud Bayesian Network for Risk Measurement. *Applied Soft Computing*, **87**, Article ID: 105947. https://doi.org/10.1016/j.asoc.2019.105947

[19] Kumar, M.S. and Raja, M.I. (2020) A Queuing Theory Model for e-Health Cloud Applications. *International Journal of Internet Technology and Secured Transactions*, **10**, 585-600. https://doi.org/10.1504/IJITST.2020.10029365

[20] Amini, M. and Bozorgasl, Z. (2023) A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology. *International Journal of Computer Science and Engineering Research*, **11**, 4-11.

[21] Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z. (2021) Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, **11**, Article No. 16. https://doi.org/10.3390/electronics11010016

[22] Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S. (2022) Cloud Computing Security: A Survey of Service-Based Models. *Computers & Security*, **114**, Article ID: 102580. https://doi.org/10.1016/j.cose.2021.102580

[23] Mondal, S.K., Pan, R., Kabir, H.D., Tian, T. and Dai, H.N. (2022) Kubernetes in IT Administration and Serverless Computing: An Empirical Study and Research Challenges. *The Journal of Supercomputing*, **78**, 1-51.

[24] Chuka-Maduji, N. and Anu, V. (2021) Cloud Computing Security Challenges and Related Defensive Measures: A Survey and Taxonomy. *SN Computer Science*, **2**, Article No. 331. https://doi.org/10.1007/s42979-021-00732-3

[25] Sun, P.J. (2019) Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *IEEE Access*, **7**, 147420-147452. https://doi.org/10.1109/ACCESS.2019.2946185

[26] Stouffer, C. (2023) 23 Cloud Security Risks, Threats, and Best Practices to Follow. https://us.norton.com/blog/privacy/cloud-security-risks

[27] Pratt-Sensie, A.A. (2020) Security Strategies to Prevent Data Breaches in Infrastructure as a Service Cloud Computing. Doctoral Dissertation, Walden University, Minneapolis.

[28] Gan, C., Feng, Q., Zhang, X., Zhang, Z. and Zhu, Q. (2020) Dynamical Propagation Model of Malware for Cloud Computing Security. *IEEE Access*, **8**, 20325-20333. https://doi.org/10.1109/ACCESS.2020.2968916

[29] González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021) Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, **21**, Article No. 4759. https://doi.org/10.3390/s21144759

[30] Abusaimeh, H. (2020) Distributed Denial of Service Attacks in Cloud Computing. *International Journal of Advanced Computer Science and Applications*, **11**, 163-168. https://doi.org/10.14569/IJACSA.2020.0110621

[31] Pontes, D. (2021, June 30) Automated, Accurate, Flexible DDoS Detection and Mitigation. https://www.kentik.com/blog/automated-accurate-flexible-ddos-detection-and-mitigation/

[32] Singh, C., Thakkar, R. and Warraich, J. (2023) IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*, **8**, 30-38. https://doi.org/10.24018/ejeng.2023.8.4.3074

[33] Tuyishime, E., Balan, T.C., Cotfas, P.A., Cotfas, D.T. and Rekeraho, A. (2023) Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. *Applied Sciences*, **13**, Article No. 12359. https://doi.org/10.3390/app132212359

[34] Mohanan, R. (2022) What Is Security Information and Event Management (SIEM)? Definition, Architecture, Operational Process, and Best Practices. https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/