Research and analysis of issues and challenges in ensuring cyber security in cloud computing

Olha Mykhaylova[1,†], Marta Korol[1,†] and Roman Kyrychok[2,*,†]

[1] Lviv Polytechnic National University, 12 Stepana Bandery str., 79013 Lviv, Ukraine
[2] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

Cloud services provide information tools in a virtual environment with the opportunity to expand the software and hardware resources of the user's computer device. Information is permanently stored on servers on the Internet and temporarily cached on client devices, such as personal computers, game consoles, laptops, smartphones, etc. To gain constant access to remote Internet resources, users use cloud services. They are a key element of rapidly evolving modern technologies, and cloud services are a strategic issue for many companies. Although the innovative capabilities of cloud services attract users, they can also create new threats to their information security. This is why research into cloud computing is important to understand its potential and effectiveness. This study will look at the security aspect of cloud services and compare several different platforms because the lack of sufficient protection can lead to the theft of personal data and other confidential information. The study will also look at the most common threats faced by cloud services, such as DDoS attacks, data leaks, data abuse, etc. In particular, the security measures provided by leading cloud platforms such as AWS, GCP, and Azure will be analyzed to determine their effectiveness and reliability. Our analysis will be useful for companies considering moving to the cloud and everyday users trying to keep their data safe online. The results of the study will provide a clear understanding of the benefits and limitations of using various cloud platforms from a security perspective.

Keywords

cloud computing security, cybersecurity in cloud services, cloud platform comparison, data protection, threats to cloud services, DDoS attack, data leakage prevention, security measures in AWS, GCP, Azure, cloud migration considerations

1. Introduction

In today's digital world, large amounts of data are stored and processed in cloud services. Cloud services are known to provide many benefits, including increased availability, flexibility, and cost-effectiveness. However, with these benefits come several challenges, such as increased security threats, potential vulnerabilities, and potential risks to data privacy [1].

In the modern world, the cloud computing market is experiencing increased competition among cloud service providers. In recent years, there has been a constant increase in the number of companies offering cloud services. The most popular of them are:

- Amazon Web Services (AWS) [2] (established in March 2006) is a division of Amazon.com that offers a cloud computing platform for rent to individuals, businesses, and governments via subscription.
- Microsoft Azure (created February 1, 2010) [3] is a Microsoft Corporation infrastructure that provides a cloud platform for application developers to facilitate the process of creating programs. Microsoft Azure allows you to deploy applications not only using Microsoft .NET and Visual Studio but also using various tools.
- Google Cloud Platform (founded April 7, 2008) [4]—a set of cloud services developed by Google, running on the same infrastructure that Google uses for its end-user products. The service provides a range of modular cloud services such as computing, data storage, data analytics, and machine learning.

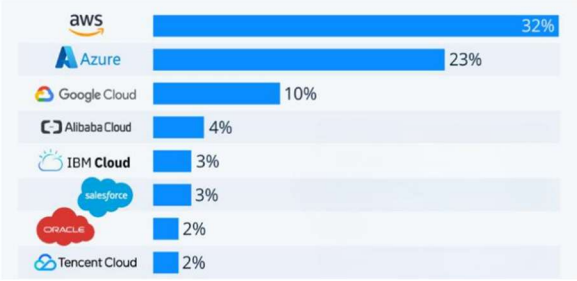

Figure 1: Popularity of cloud service providers [5].

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
olha.o.mykhailova@lpnu.ua (O. Mykhaylova);
marta.korol.kb.2022@lpnu.ua (M. Korol);
r.kyrychok@kubg.edu.ua (R. Kyrychok)

0000-0002-3086-3160 (O. Mykhaylova);
0009-0002-8079-1799 (M. Korol);
0000-0002-9919-9691 (R. Kyrychok)

With increasing popularity, developers are forced to constantly improve their platforms, including improving automatic threat detection and response mechanisms, expanding data encryption capabilities, improving user identification and authentication, and improving monitoring and vulnerability analysis tools [6]. Collaborate with information security experts, conduct independent security audits, and improve incident response processes.

The topic of cloud computing has attracted the attention of various researchers. Many scholars and experts are actively engaged in research and analysis of the problems and challenges associated with cybersecurity in cloud computing. Using an example, work [7] examines security in the AWS computing service; it demonstrates the importance and relevance of research in the field of cybersecurity, in particular in the context of the use of AWS cloud services. Also, in [8], the authors compared AWS and Azure Cloud Platforms services for 2021, where they recognize the differences between AWS and Azure in database management systems, architectures, resource management patterns, and complexity, which can affect scalability, performance, and pricing.

The method of this research is to analyze and identify the key issues and challenges that are used in cybersecurity inactivity processes in external computing to further align Amazon Web Services, Microsoft Azure, and Google Cloud Platform. To do this you will also need to use:

- Updated downloads and resources without additional services
- Identify non-response criteria in general descriptions.
- Test AWS, AZURE, and GCP in the context of selected cybersecurity blocking criteria.
- Evaluate each platform on 10 balloon systems
- Focus on the platform that is effective and relevant.

Thus, reviewing and analyzing the issues and challenges associated with cybersecurity in general terms remains extremely important for developing effective data preservation strategies.

2. Analysis of threats and security risks of cloud services

Small and medium-sized enterprises, like global companies, are increasingly relying on cloud computing security services to support day-to-day business functions and software development, and even to provide the technology infrastructure needed to operate. In this regard, cloud services often face many cyber-attacks.

A cloud attack [9] is a cyber-attack that targets cloud service platforms, such as computing services, storage services, or hosted applications in a platform as a service (PaaS) or software as a service (SaaS) model.

According to [10], in recent years the number of attacks on cloud services has increased rapidly. Cloud cyberattacks accounted for 20% of all cyberattacks in 2020, making cloud computing platforms the third most targeted cyber environment. Therefore, we will look at the different types of attacks and their characteristics, as well as the possible consequences of these attacks for users and organizations using cloud technologies. Below is an overview of types of cloud computing attacks to help you better understand these threats and take steps to prevent them.

These threats pose serious risks to cloud computing security. Denial-of-service attacks can disrupt access to cloud services, misconfiguration of security can open the door to attackers, and cloud malware attacks threaten data privacy and integrity. This may allow an attacker to use the associated resources for their purposes or to steal or manipulate data stored in the cloud. All these threats require important monitoring and the provision of appropriate security measures to protect cloud services and user data.

2.1. Denial of service in cloud computing

DoS attacks attempt to make a service unavailable to its users. The attack consumes a large amount of system resources such as computing power, memory, and bandwidth. This consumption will make the service unavailable to users or unbearably slow.

DoS attacks and their variant distributed denial of service (DDoS) attract a lot of media attention mainly because of their magnitude. In 1988, reports show only six DDoS attacks. DDoS attacks targeted major websites such as CNN, Yahoo, and Amazon in 2000 with an attack rate of approximately 1 GB/s. DDoS attacks achieved a speed of 70 GB/s in 2007. In 2013, there was a large-scale attack on a service. Over the past decade, DDoS attacks on cloud services have become increasingly sophisticated and dangerous, affecting various industries and operations related to cloud resources [11].

The attack on Spamhaus in 2013 stands out for its scale, using a traffic volume of 300 Gbps, which led to disruptions not only to Spamhaus itself but also to global Internet traffic.

A politically motivated attack on GitHub in 2015 showed the use of compromised devices to flood the website with traffic and disrupt its operations.

A 2016 Dyn attack that used compromised IoT devices to create a botnet overwhelmed Dyn's infrastructure, causing major sites like Netflix and PayPal to become unavailable.

Attacks on Google and AWS in 2020, using amplification techniques, resulted in extremely high traffic speeds (2.5 Tbsp. for Google and 2.3 Tbsp. for AWS), which posed a major threat to their infrastructure [12].

In 2022, Microsoft discovered protection against extremely high-throughput attacks, registering the largest attack at the time at 3.47 Tbit/s. Also noted is the shift to multi-vector attack strategies, where attackers combine different methods to maximize disruption.

Look closer at DoS attacks, which occur when security is compromised. This prevents legitimate clients from accessing its target cloud systems, devices, or other cloud resources.

A network of zombies controlled remotely by well-structured and widely distributed nodes perform DDoS attacks. The attacker initiates the attack with the help of zombies called secondary victims. DDoS attacks are divided into 3 categories [12].

1. Volume/Bandwidth-Based Attacks: This attack tries to overwhelm the user with a lot of garbage

data, using network bandwidth and resources in the process.
2. Protocol attacks: The attack tries to overload the target's resources using the disadvantage associated with several network protocols.
3. Application Layer Attacks: These attacks target specific online applications and send HTTP requests that exceed program capacity.

2.2. Account Hijacking

In this type of security breach, hackers attempt to hijack an account by stealing security credentials and then eavesdropping on user actions and transactions.

Hackers can also manipulate data, insert false information, and redirect customers to illegitimate sites. This type of vulnerability is particularly scary because hackers know how to use the reputation and trust of users to manipulate customers.

In 2010, Amazon faced an attack [12–14] that allowed hackers to steal the session IDs that give users access to their accounts after entering passwords. This left the customer's credentials open to hackers. The bug was removed 12 hours after it was discovered, but many Amazon users were unwittingly exposed to the attack during that time [15].

Account hijacking is done using the stolen credentials of the real user. By using credentials a hacker can access sensitive data and manipulate the data to suit his likeness. The traffic hijacking service involves hacker eavesdropping, data manipulation, data access, and return of falsified information. There are three states in which a security breach can occur.

1. Transfer of confidential data to a cloud server.
2. Transfer of confidential data from the cloud server to the client's computer.
3. Storage of confidential client data in the cloud servers that are remote and not owned by the client [16].

In account hijacking, a hacker uses a compromised email account to impersonate the account owner. Typically, account hijacking is done through phishing [17], sending fake emails to the user, picking a password, or several other hacking tactics. In many cases, a user's email account is linked to various online services, such as social networks and financial accounts.

A hacker can use an account to obtain a person's account personal information, conduct financial transactions, create new accounts, and request the account owner's contacts for money or assistance in illegitimate activities. Cloud account hijacking is a common tactic for identity theft schemes. The attacker uses the stolen account information for malicious or unauthorized activity. When a cloud account is hijacked, the attacker usually uses a compromised email account or other credentials to impersonate the account owner.

Hijacking an enterprise-level cloud account can be particularly devastating, depending on what the attackers do with the information. A company's integrity and reputation can be destroyed, and confidential data can be destroyed by leakage or falsification, causing significant costs for businesses. There are also possible legal consequences for companies and organizations with strict regulation industries, such as healthcare, if sensitive customer or patient data is exposed when a cloud account is compromised [14].

2.3. Malware injection in cloud computing

Malware injection in cloud computing is when an attacker tries to step in and inject malicious code or a fake service that masquerades as an existing service running in the cloud. This type of attack is also known as a download or metadata spoofing attack. Attacks of this type allow attackers to steal information from the Internet by causing automatic downloads of malicious software without prior consent from users. This undermines the reliability of the service and may lead to unwanted behavior. This may be the first serious attack attempt to introduce a malicious service or virtual machine in a cloud environment [11].

The goal of a cloud-based malware attack is to harm anything of interest, which may include data modification, functionality/behavior modification, or blocking. In such an attack, an attacker creates his implementation of a malicious service or module (for example, SaaS or PaaS) or a virtual machine instance (for example, IaaS) and adds it to a cloud system. The attacker then pretends to the cloud system that it is a new service or implementation instance among the valid instances for the service being attacked. If this action is successful, the cloud automatically redirects the valid user's requests to the implementation of the malicious service and the malicious code is executed. The basic cloud ware Injection attack scenario is that an attacker transfers a manipulated/incorrect copy of a service instance to the victim so that the malicious instance can access the victim's service requests. To achieve this goal, the attacker must gain control over the victim's data in the cloud [11].

An SQL injection attack is aimed at a database that is outside the client's input fields in the application. A malicious SQL command is inserted as part of an information field, which, when changed to a query, turns it into a meaningful, but unsafe, query.

A Cross-Site Scripting (XSS) attack is where an attacker gains access to sensitive information on the server by injecting code into the context of the document data used on the client-side HTML. This method allows the attacker to execute his script in the victim's web browser. XSS attacks are classified as stored and displayed according to OWASP. According to WHID (2011), about 12.6% of all attacks on the Internet are related to XSS. There is virtually no limit to the various XSS-based attacks.

A command injection attack is a form of command injection in which commands entered by vulnerable programs are executed. These entered commands can be executed at the root level or in a separate runtime environment, depending on the conditions. The commands entered, such as ls, ps, cat, etc., are executed in the context of the running environment with similar privileges as the application being used. One of the most important consequences of this attack is increased latency for alternate clients using applications running on the same virtual machine as the vulnerable application [11].

2.4. Insecure APIs

The API plays a crucial role in the communication of the cloud computing infrastructure because it allows different users and cloud components to interact and share data. Thus, an attacker can exploit weaknesses in cloud management software such as Open Stack and its API implementation for malicious intent [18, 19].

The first type of attack is an attack on API authentication services. This type of attack can be initiated by exploiting weaknesses in the cloud API that provides authentication services in the cloud infrastructure. Cloud management software such as OpenStack or CloudStack has provided an API to interact with authentication services. The relationship between hosts and authentication is sensitive because credentials such as passwords and session tokens are usually exchanged during the session.

Most APIs in cloud management software are based on REST or SOAP, which are web standards [20]. Thus, it is vulnerable to Internet-based attacks such as eavesdropping, session hijacking, malicious code execution, XSS, and denial-of-service attacks [20]. One important OpenStack service is the API that handles authentication, a module known as Keystone. Work [21] revealed that the Keystone API is also susceptible to eavesdropping attacks because, during the authentication procedure, credential data is transmitted to users in clear text. Additionally, Keystone's token exchange-based authentication mechanism is also flawed. This is because hackers will be able to gain user privileges and access the services of other cloud components if they can get the password contained in the authentication token [18, 19].

The second type of attack is the API Exhaustion Attack. This is a type of DOS attack on cloud API services. A denial of service (DOS) occurs when an attacker disrupts services by intentionally sending a large volume of traffic to overload the system. This prevents the system from processing the request of legitimate users and thus denying them access to the service. In the context of cloud computing, a DOS attack can target applications running in the cloud or the infrastructure of the cloud platform [22, 23].

When a DOS attack targets a cloud platform API, it can cause an API exhaustion attack. Most cloud management software offers a web API for interoperability and simplicity. For example, CloudStack and OpenStack APIs are built on REST, and during a communication session, data is formatted as JSON [24, 25]. Work [21] found that the OpenStack Keystone API, which uses web protocols to provide identity and authentication services, is vulnerable to information disclosure, DOS, and replay attacks.

An API exhaustion attack is when attackers maliciously exploit a cloud platform's API by sending many malicious API requests to overload the system. Cloud components will not be able to respond to legitimate API requests from other components and users while it is full. This is because web protocols (HTTP) use TCP as the transport protocol, thus, when the server receives API requests using HTTP; it will allocate additional resources for a new TCP session. The physical hosts of the cloud management system components will eventually wear out if this continues for a long period. Therefore, it cannot handle a legitimate API request, resulting in a DOS attack and violation of its availability. Cloud management software is vulnerable to this type of attack because it uses web technology in API services and many cloud administrators have drawn attention to this problem bug tracking portal and vulnerability database [15, 20].

2.5. Security misconfiguration

The latest report highlights that 75% of medium and large companies have switched to cloud computing. However, misconfiguration errors remain a major security concern in cloud computing. These errors are often the result of human errors that can occur when configuring cloud instances such as compute resources and storage, which can increase the system's vulnerability to data security breaches [26].

For example, improper configuration of an Amazon S3 instance can lead to improper access to protected documents via a web browser. This problem extends to insecure data stores on the Internet without any form of authentication, allowing all users of the platform to access the data. These errors impact the ability of cloud administrators to adequately control and secure complex hybrid and multi-cloud deployments [18].

Various factors can lead to misconfiguration errors. For example, a lack of understanding of cloud security policies, congestion, and misuse of APIs can complicate this situation. Ensuring that software components have proper default security settings is also an important reason, which facilitates the attempts of attackers to gain access to data. All this shows that misconfiguration errors can have serious consequences for data security in cloud environments [25].

3. Cybersecurity assessment criteria in cloud computing

Given that cyberattacks are becoming more sophisticated and cybersecurity threats are constantly growing, the importance of developing a comprehensive security strategy for cloud services becomes imperative. For effective protection against cyberattacks in cloud services, it is recommended to use a variety of measures and protection methods that allow to guarantee a higher level of security for users.

3.1. Security misconfiguration

While AWS, Azure, and Google Cloud are the leading cloud service providers, they each have specific mechanisms in place to ensure cybersecurity.

One of the key mechanisms is access demarcation and security management in the cloud computing environment.

Identity and Access Management (IAM) allows you to create and manage permissions for resources. IAM combines access control to services into a single system and is a consistent set of operations. IAM policies contain a role, user, or user group. Each role contains a list of permissions.

Identity and access management is based on such principles as:

- Multi-factor authentication adds an extra layer of security. This means that a user will need to verify their identity using two or more authentication

methods, such as a password and an SMS code, to access your account.

- Centralized management, with which users can create and manage access policies for users, groups, and roles from one place, which simplifies the administration process.
- Role-based Access Control (RBAC) allows you to define access rights for users based on their responsibilities and needs. This allows you to fine-tune access to resources based on the specific needs of your organization.
- IAM provides auditing and reporting capabilities that allow you to log access events, analyze resource usage, and track changes to access policies to meet regulatory requirements. This allows you to maintain control over your data and ensure compliance with security standards.

The main conclusions of our research include:

Algorithm Development: A new algorithm based on the Taylor series has been proposed that provides the generation of pseudorandom sequences. This approach is based on the numerical properties of the natural logarithm of number 2 (ln2), which is mathematically stable and accurate. Using ln2 to initialize the generator allows achieving a high degree of randomness in the created sequences.

Algorithm Analysis: A detailed analysis of the developed algorithm was conducted, which includes checking its statistical characteristics and testing for compliance with NIST requirements. Testing showed that the algorithm could not initially provide a uniform distribution of pseudorandom numbers, leading to its improvement.

Algorithm Improvement: The basic algorithm has been improved, which provides better performance and improved statistical characteristics of the generated sequences. Optimization of the algorithm allows for significantly reducing the computational complexity, making it effective for use in real-world applications where computation time is a critical parameter.

The results of this research are an important step towards improving the reliability and quality of pseudorandom number generators. The proposed approach may find wide application in various fields such as cryptography, numerical modeling, simulations, and other numerical methods that require high-quality randomness and computational efficiency.

Furthermore, the improved algorithm proposed in this paper can be used to create new generators or to enhance existing solutions, for example through optimization of calculations or application of new generation methods. Future research may focus on expanding the algorithm to other mathematical constants, which may further improve the quality of pseudorandom numbers. It is also possible to create an algorithm based on formula (5) using intervals (for example, as in Hamming matrices) or using other Taylor series for generating new pseudorandom sequences. Using such methods opens new horizons for the development of number theory and computational mathematics, providing powerful tools for solving a wide range of tasks in various fields of science and technology, especially for information protection.

3.2. Protection against DDoS attacks and other network threats

One of the most common and most threatening forms is a DDoS (Distributed Denial of Service) attack, which can cause significant disruption to work networks, lead to the loss of availability of services and important data, and even cause significant financial losses. Protection against a DDoS attack is based on the following points [26–28]:

- Scalability and elasticity of the infrastructure
- Distribution
- Network filters
- Traffic optimization
- Monitoring and analytics services.

3.3. Measures to prevent unauthorized data changes

In the world of cloud services, where data security is important, preventing unauthorized changes to information becomes an important task. Ensuring data privacy requires the implementation of effective security measures. In this context, it is important to note the measures to prevent data changes without permission, which becomes the main component of information reliability and security.

In cloud services, several functions and mechanisms help avoid data changes without permission:

- Auditing and monitoring: Auditing and monitoring systems provided by cloud providers can track all activities with data and resources. Some threats and unusual activity are detected in time.
- Data encryption: Data encryption features such as AWS Key Management Service, Google Cloud Key Management Service, and Azure Key Vault can protect data from unauthorized access even if attackers gain access to it.
- Tracking changes: Some cloud services provide the ability to track changes in data using audit logs. This allows you to identify who, when, and what changes were made to the data.
- Backup: Backup features offered by regular cloud providers can back up data and restore it in case of unauthorized changes or loss.

3.4. The shared responsibility model

The shared responsibility model is a concept that defines the level of responsibility for security and data protection between a cloud service and its customers. This model chooses who is responsible for various aspects of infrastructure and data in a cloud environment.

Also, choose 1 of 3 types of platform services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

SaaS [29] is a model that puts the most responsibility on the cloud service provider and the least on the user. In a SaaS environment, you are responsible for the data you add

to the systems, the devices you allow to connect to the systems, and the users who have access. Almost everything else belongs to the cloud provider. The cloud provider is responsible for the physical security of the data centers, power, network connectivity, and application development and updates [30].

PaaS [31] divides the responsibility between you and the cloud provider. The cloud provider is responsible for maintaining the physical infrastructure and its access to the Internet, just like in IaaS. In the PaaS model, the cloud provider also supports operating systems, databases, and development tools. Think of PaaS as using a domain-joined computer: IT staff maintain the device with regular updates, patches, and upgrades.

IaaS places the greatest responsibility on the user. The cloud provider is responsible for maintaining the physical infrastructure and its access to the Internet. You are responsible for installation and configuration, patches and updates, and security.

3.5. The shared responsibility model

The availability and effectiveness of security policies is one of the most critical aspects. Well-designed security policies can protect against a wide range of threats, from cyber attacks to unauthorized access and data loss. They define the rules, procedures, and controls that govern access to information and resources, and establish security standards that must be followed by all users and system administrators. In this context, it is important to investigate both the presence and effectiveness of security policies in cloud services to ensure a high level of data and infrastructure protection.

Criteria for determining its effectiveness and adaptability to security requirements include:

The assessment of the security policy in cloud services includes several criteria that allow for determining its effectiveness and adaptability to security requirements. Some of the key evaluation criteria include:

- Certainty and consistency.
- Compliance The security policy must meet the requirements of legislation, standards, and regulatory requirements that apply to a specific industry or region.
- Monitoring and analysis.
- Sustainability and renewal.
- Support and involvement of employees.

Evaluating a security policy against these criteria helps ensure that it meets the needs and requirements of security in cloud services.

4. Conducting testing of each platform according to defined criteria

Taking into account the criteria of the Criteria for evaluating cyber security in cloud computing, which were compiled in the previous points, we will compare 3 cloud services: AZURE, AWS, and GCP.

Table 1
Platform comparison in the context of access demarcation

Criterion/Platform	AWS	AZURE	GCP
Multi-factor Authentication	Yes, supported through IAM and other services	Yes, including Azure AD and other mechanisms	Yes, available to users and services through the Identity Platform
Centralized Management	Yes, through Identity and Access Management (IAM)	Yes, via Azure Active Directory (AAD) and other tools	Yes, with Cloud Identity and Access Management (IAM)
Role-based Access Control	Yes, roles and access rights can be defined through IAM	Yes, through Azure RBAC and other mechanisms	Yes, available for configuring access rights for users and services
Audit and Reporting	Yes, provides capabilities for logging events and resource usage analysis	Yes, provides audit and reporting capabilities through Azure Monitor and other tools	Yes, provides capabilities for logging events and analyzing resource access

Evaluating access separation for each of the platforms (Azure, AWS, GCP) on a scale from 1 to 10, where 10 is the best, you can make the following rating:

1. Azure (Microsoft Azure): 8. The service has a powerful and easy-to-use access control mechanism through Azure Active Directory (AAD). It provides the ability to manage many built-in roles, but some functionality can be difficult to configure with other platforms.
2. AWS (Amazon Web Services): 9. IAM in AWS is a powerful and flexible tool for delimiting access. It provides extensive configuration options for roles, policies, and API access. Many built-in roles and categories refused to fine-tune access to resources.
3. GCP (Google Cloud Platform): 7. IAM in GCP is also a powerful access management tool, but it can be less flexible in some aspects together with AWS and Azure. However, it provides advanced functionality for managing projects and resources.

Then we compare platforms with points of protection against DDoS attacks and other network threats:

Table 2
Comparison of platforms in the context of protection against DDoS attacks and other network threats

Criterion/Platform	AWS	Azure	GCP
Free Basic Level of DDoS Protection	Yes, available to all users	Yes, through Azure DDoS Protection	No
Enhanced Protection for an Additional Fee	Yes, available through AWS Shield Advanced	No, enhanced protection is not available for an additional fee	Yes, available through Google Cloud Armor and other mechanisms
Web Application Firewall (WAF)	Yes, AWS WAF	No, but Azure Firewall and Azure Security Center are available	Yes, Google Cloud Armor
Event Logs and Security Analysis	Yes, available through AWS CloudTrail and AWS Config	Yes, available through the Azure Security Center	Yes, available through the Google Cloud Security Command Center

Having familiarized ourselves with the platforms in terms of protection against DDoS attacks and other network threats, we can give them the following ratings:

1. AWS (Amazon Web Services): 9. AWS provides a high level of protection against DDoS attacks and other network threats, including services such as AWS Shield, AWS WAF, AWS Firewall Manager, Amazon GuardDuty, and others. These services provide different levels of protection, both basic and advanced, allowing you to adapt protection measures to the needs of users. Multi-factor authentication, protection of network resources, and tracking of unusual activity are also components of AWS security systems.
2. Azure (Microsoft Azure): 8. Microsoft Azure also offers a wide range of tools to protect against DDoS attacks and other network threats, including services such as Azure DDoS Protection, Azure Firewall, Azure Application Gateway, Azure Security Center, and many others. Azure has a well-developed threat monitoring and detection system that allows you to quickly respond to any attacks.
3. GCP (Google Cloud Platform): 7. Google Cloud Platform provides a significant level of protection against DDoS attacks and other network threats with services such as Google Cloud Armor, Google Cloud DDoS Protection, VPC Service Controls, and others. However, according to some experts, GCP's security tools may be less integrated and less easy to use with AWS and Azure, which may pose some risk to users with less expertise in network security.

Below is a table that compares measures to prevent unauthorized data changes across AWS, Azure, and GCP based on criteria such as auditing and monitoring, data encryption, change tracking, and backup:

Table 3
Comparison of platforms in the context of measures to prevent unauthorized data changes

Criterion/Platform	AWS	Azure	GCP
Tools and services	IAM, AWS Shield, AWS WAF, and other	Azure Active Directory (AAD), Azure DDoS Protection, and other	GC IAM, GC Armor, Google Cloud Security Command Center, and other
Service Models	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS
Security Policies and Standards	Uses own security policies and standards, such as PCI DSS, HIPAA, SOC, ISO	Uses own security policies and standards, such as PCI DSS, HIPAA, SOC, ISO	Uses own security policies and standards, such as PCI DSS, HIPAA, SOC, ISO, and others

The evaluation schedule can be justified as follows:

1. AWS (Amazon Web Services): Score 9. AWS has several powerful tools such as IAM for access management, AWS KMS for data encryption, CloudTrail for auditing and monitoring, and Amazon S3 for backup. These tools provide extensive opportunities for data protection and a high level of security.
2. Azure (Microsoft Azure): Score 8. Azure also has a similar set of data protection tools, such as Azure Active Directory, Azure Key Vault, Azure Audit Logs, and Azure Backup. However, some users may find Azure a bit more difficult to configure and use, which may result in a slight loss of points compared to AWS.
3. GCP (Google Cloud Platform): Score 7. GCP also has some effective data protection tools but may be less flexible in some aspects compared to AWS and Azure. While tools like Cloud IAM, Key Management Service, and Cloud Audit Logs offer a high level of security, GCP's interface and documentation may be less intuitive for some users, which lowers the overall score.

Next, the aspect of the joint responsibility model will be considered.

Table 4
Comparison of platforms in the context of shared responsibility models

Criterion/Platform	AWS	Azure	GCP
Audit and Monitoring	AWS CloudTrail, Amazon CloudWatch	Azure Monitor, Azure Security Center	Cloud Audit Logs, Cloud Monitoring
Data Encryption	AWS Key Management Service (KMS), Amazon S3 Encryption	Azure Key Vault, Data Encryption at Rest	Key Management Service, Data Encryption at Rest
Change Tracking	AWS CloudTrail	Azure Audit Logs	Cloud Audit Logs
Backup	Amazon S3, Amazon Glacier	Azure Backup	Google Cloud Storage, Cloud Storage Nearline

The evaluation schedule can be justified as follows:

1. Azure (Microsoft Azure): 9. Azure provides a well-defined shared responsibility model that chooses which parts of the infrastructure are the responsibility of the cloud provider and which are the responsibility of the user. This will avoid confusion and understand the responsibilities of all parties for data and infrastructure security.
2. GCP (Google Cloud Platform) 8. GCP also provides a shared responsibility reporting model, but some users feel that some aspects may be less obvious or difficult to understand with Azure or AWS.
3. AWS (Amazon Web Services): 9. AWS has a well-defined and reported shared responsibility model that allows users to clearly understand their responsibility for the security and protection of data in the cloud environment.

Table 5
Comparison of platforms in the context of shared responsibility models

Criterion/Platform	AWS	Azure	GCP
Availability of Certifications	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP
Virtualization Support	AWS Config, AWS Inspector, AWS Trusted Advisor	Azure Security Center, Azure Policy, Azure Firewall	Google Cloud Security Command Center, Google Cloud IAM, Google Cloud Armor

The evaluation of the effectiveness of security policies in different cloud platforms can be as follows:

1. Azure (Microsoft Azure) 9. Azure provides extensive capabilities for creating and configuring security policies through Azure Security Center and Azure Policy. Thanks to these services, administrators can effectively control and monitor the state of security of resources in the Azure cloud environment. Azure also provides opportunities for integration with other security monitoring and management systems, which increases its effectiveness.
2. GCP (Google Cloud Platform) 8. GCP also has an extensive set of tools for configuring security policies, including Cloud Security Command Center and Google Cloud IAM. However, some users may find GCP's user interface and documentation to be less intuitive compared to Azure or AWS, which can make it difficult to set up and debug security policies.
3. AWS (Amazon Web Services): 9. AWS offers a wide range of tools for creating and managing security policies, including AWS Identity and Access Management (IAM), AWS Config, AWS CloudTrail, and many others. These services allow administrators to effectively control and monitor the security of resources in the AWS cloud environment.

Table 6
Comparison of platforms in the context of shared responsibility models

Criterion/Platform	AWS	Azure	GCP
Access Control	9	8	7
Protection from DDoS and Other Network Threats	9	8	7
Measures to Prevent Unauthorized Data Changes	9	8	7
Shared Responsibility Models	9	9	8
Effectiveness of Security Policies	9	9	8
Overall Score	45	42	37

From the ratings provided, it can be noted that Amazon Web Services (AWS) received the highest overall rating, which is 45 points. This is a subjective opinion that was built on the fact that AWS stands out in terms of technical aspects with its broad set of services, deep level of customization, and high geographical spread. The biggest advantage of AWS is a powerful and selective toolkit for delimiting access, as well as a wide range of tools to protect against DDoS attacks and other network threats. Considering this, it can be concluded that AWS is the best choice for organizations that want optimal security in cloud computing.

5. Conclusions

Based on the research and analysis of the issues and challenges associated with ensuring cyber security in cloud computing, several key conclusions can be drawn.

First of all, it is determined that protection against cyber threats in cloud computing requires a comprehensive and in-depth approach, the latter areas provide a wide range of services and capabilities that require constant monitoring and management. Key challenges in this context include ensuring data security and protection, detecting and responding to cyber threats, and managing access and user identity.

Another aspect of security is the continuous updating and improvement of security measures since cyber threats are constantly evolving and remain increasingly complex. This means that cloud computing providers such as AWS, Azure, and GCP must constantly improve their tools and services to ensure the highest level of security for their customers.

In addition, it is found that the choice of cloud computing platform can affect the level of cyber security, the second provider has its unique features and capabilities. The decisive factor when choosing a platform should be its ability to provide reliable and effective protection against cyber threats to the needs and requirements of a specific organization.

Therefore, based on these findings, it can be argued that ensuring cyber security in cloud computing is a challenging task, but at the same time, there are ample opportunities for innovation and development. With an understanding and timely response to the problems and challenges in this area, organizations can maximize the security of their data.

References

[1] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7390–7404.

[2] Sabahi, F., & Movaghar, A. (2023). A Survey on Cloud Computing Security: Challenges and Opportunities. IEEE Access, 11, 34501-34519. doi: 10.1109/ACCESS.2023.3258591

[3] Kumar, P., Singh, G., & Rathore, S. (2023). Cloud Computing Services and Platforms: A Detailed Review and Future Perspectives. Future Generation Computer Systems, 143, 1023-1038. doi: 10.1016/j.future.2023.07.003

[4] M. A. Shah, M. Khan, M. Ahmed, Cloud Computing: Principles, Systems and Applications. Springer (2023). doi: 10.1007/978-3-031-25711-2

[5] F. Richter, Worldwide Market Share of Leading Cloud Infrastructure Service Providers (2024). URL: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

[6] Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing

[7] V. M. Mazur, Assessment of the Security of the Use of Cloud Technologies and the Development of Methods of Protection Against Cyber Attacks on Cloud Services, Ternopil: TNTU (2023).

[8] S. Galiveeti, et al., Cybersecurity Analysis: Investigating the Data Integrity and Privacy in AWS and Azure Cloud Platforms, Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Studies in Big Data, 90 (2021) doi: 10.1007/978-3-030-74575-2_17.

[9] A. Sheps, Top 10 Cloud Attacks and What You Can Do About Them (2023). URL: https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

[10] Triskele Labs, Cloud Cyber Attacks: The Latest Cloud Computing Security Issues. URL: https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues

[11] P. Kumar, Cloud Computing: Threats, Attacks and Solutions, Int. J. Emerging Technol. Eng. Res. (IJETER), 4(8) (2016) 24–28.

[12] A. V. Songa, A Review of DDoS Attacks and its Countermeasures in Cloud Computing, in International Conference on Information Systems and Computer Networks (2022). doi: 10.1109/ISCON52037.2021.

[13] A. A. Christina, Proactive Measures on Account Hijacking in Cloud Computing Network, Asian J. Comput. Sci. Technol. 4(2) (2015) 31–34.

[14] I. Ranjan, R. Bhushan, Ambiguity in Cloud Security with Malware-Injection Attack, in: 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA) (2019) 1–5. doi: 10.1109/ICECA.2019.8821844.CClo.

[15] D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 217–225.

[16] Y. Martseniuk, et al., Automated Conformity Verification Concept for Cloud Security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 25–37.

[17] O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398–409.

[18] O. Vakhula, I. Opirskyy, O. Mykhaylova, Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 55–69.

[19] CWE: Individual Dictionary Definition. “Improper Neutralization of Special Elements used in a command” (2017) 209–217.

[20] F. Qazi, Application Programming Interface (API) Security in Cloud Applications, EAI Endorsed Transactions on Cloud Systems, 7(23) (2023) e1. doi: 10.4108/eetcs.v7i23.3011.

[21] H. Albaroodi, S. Manickam, P. Singh, Critical Review of Openstack Security: Issues and Weaknesses, J. Comput. Sci., 10(1) (2014) 23–33.

[22] M. Ali, et al., Mobile Cloud Computing with SOAP and REST Web Services, Journal of Physics: Conference Series, 1018 (2018) 012005. doi: 10.1088/1742-6596/1018/1/012005.
[23] J. Somorovsky, et al., All Your Clouds Are Belong to Us, in: 3rd ACM workshop on Cloud computing security workshop – CCSW'11 (2011).
[24] B. Cui, T. Xi, Security Analysis of Openstack Keystone, in: 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (2015).
[25] O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 29–43.
[26] C. N. Nobles, Investigating Cloud Computing Misconfiguration Errors using the Human Factors Analysis and Classification System, Scientific Bulletin 27(1) (2022). doi:10.2478/bsaft-2022-0007.
[27] Developer.openstack.org. OpenStack Docs: OpenStack APIs (2016). URL: http://developer.openstack.org/api-guide/quick-start/api-quick-start.html#openstack-api-quick-guide
[28] S. Goasguen, Intro to CloudStack API, Slideshare.net (2013). URL: http://www.slideshare.net/sebastiengoasguen/intro-to-cloudstack-api.
[29] A. Alkahtani, M. A. Khan, S. Hariri, A Comprehensive Survey on Cloud Computing Service Models. IEEE Access, 11 (2023) 34792–34810. doi: 10.1109/ACCESS.2023.3262599
[30] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 240–245.
[31] M. Silic, A. Back, A Comparative Study of PaaS and SaaS Cloud Models: Current Trends and Future Directions. J. Cloud Comput. Adv. Syst. Appl., 12(1) (2023) 14–28. doi: 10.1186/s13677-023-00211-8