UDC 004.056.5, 004.7, 004.738.5, 004.8
DOI: 10.18799/29495407/2024/2/50

Comparative analysis of security models in cloud platforms

S.M. Levin✉

Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation

✉semen.m.levin@tusur.ru

Abstract. This article is dedicated to the importance of data security on cloud platforms, highlighting the subject relevance in an era where threats to information security are becoming increasingly complex and sophisticated. The primary focus is a comparative analysis of security models employed by leading cloud platforms such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, and Oracle Cloud. The research covers various crucial security aspects, including data encryption, identity and access management, monitoring mechanisms and incident response. The article sheds light on current trends and technologies in cloud data protection, including the use of artificial intelligence and machine learning to enhance threat detection efficiency and the implementation of confidential computing and blockchain technologies to improve data protection. Issues of compliance with legal requirements and data security standards are discussed, along with recommendations for organisations to optimise information protection in the cloud environment.

Keywords: cloud technologies, data security, cyber threats, data encryption, access management, security monitoring, Artificial Intelligence in security, blockchain in data protection, compliance with regulatory requirements, adaptive security systems

For citation: Levin S.M. Comparative analysis of security models in cloud platforms. *Bulletin of the Tomsk Polytechnic University. Industrial Cybernetics*, 2024, vol. 2, no. 2, pp. 1–16. DOI: 10.18799/29495407/2024/2/50

УДК 004.056.5, 004.7, 004.738.5, 004.8
DOI: 10.18799/29495407/2024/2/50
Шифр специальности ВАК: 2.3.8

Сравнительный анализ моделей безопасности в облачных платформах

С.М. Левин✉

Томский государственный университет систем управления и радиоэлектроники, Россия, г. Томск

✉semen.m.levin@tusur.ru

Аннотация. Статья рассматривает вопросы безопасности данных в облачных платформах, подчеркивает актуальность темы в условиях, когда угрозы информационной безопасности становятся все более сложными и изощренными. Основное внимание уделено сравнительному анализу моделей безопасности, применяемых ведущими облачными платформами, такими как Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud и Oracle Cloud. Исследование охватывает ряд ключевых аспектов безопасности, включая шифрование данных, управление идентификацией и доступом, а также механизмы мониторинга и реагирования на инциденты. В статье освещены современные тенденции и технологии в области защиты облачных данных, в том числе использование искусственного интеллекта и машинного обучения для повышения эффективности обнаружения угроз, а также применение конфиденциальных вычислений и блокчейн-технологий для улучшения защиты данных. Обсуждается вопрос соответствия моделей безопасности платформ стандартам безопасности данных, а также предлагаются рекомендации для организаций по оптимизации защиты информации в облачной среде.

Ключевые слова: облачные технологии, безопасность данных, киберугрозы, шифрование данных, управление доступом, мониторинг безопасности, искусственный интеллект в безопасности, блокчейн в защите данных, соответствие нормативным требованиям, адаптивные системы безопасности

Для цитирования: Левин С.М. Сравнительный анализ моделей безопасности в облачных платформах // Известия Томского политехнического университета. Промышленная кибернетика. – 2024. – Т. 2. – № 2. – С. 1–16. DOI: 10.18799/29495407/2024/2/50

Introduction

Cloud technologies are critical in the modern world, where digital transformation encompasses all aspects of business and daily life. Cloud platforms provide robust and scalable solutions for storing, processing, and analysing data, offering flexibility and cost savings. However, as more organisations and individual users rely on cloud services for storing and processing their data, data security issues become increasingly pertinent and complex [1, 2].

The market offers a multitude of cloud platforms, each proposing its set of tools and security measures to protect user data [3]. These security measures are devised in response to current threats and anticipation of potential future attacks. Modern security models in cloud platforms must be flexible and adaptive to meet users' and businesses' diverse and ever-changing requirements [4].

It should be noted that the widespread adoption of cloud technologies raises the level of complexity in data security management [5]. With the storage and processing of critical corporate and personal information on external servers, data security issues become a priority [6]. The increasing number of cyber threats and strict requirements for compliance with regulatory acts in information protection drive the importance of protecting data on cloud platforms [7]. Security breaches can lead to significant financial losses, damage to reputation, and legal consequences for organisations [8].

Today, cloud providers offer a wide range of tools and services to ensure the security of stored and processed data [9]. However, the responsibility for data protection rests not only with cloud service providers but also with the users of cloud platforms themselves. Adequate data protection in the cloud requires a comprehensive approach, including proper access policy configuration, data encryption, multi-factor authentication, and regular security audits [10].

The relevance of the data security topic in cloud platforms is conditioned by the constant development of technologies and the evolution of cyber threats [11]. New methods of attack necessitate the development of advanced protection mechanisms and the adaptation of existing security approaches [12]. In this context, understanding modern trends and technologies in security provision becomes a key factor in successful digital transformation and reliable protection of valuable information [13].

This article presents an overview and comparative analysis of security models used by leading cloud platforms.

Literature review

Numerous studies have been conducted on cybersecurity and data protection on cloud platforms, covering various aspects – from threat models and attack vectors to specific encryption technologies and security standards. The literature review presented herein aims to systematise the existing scientific works in this area, identifying key trends and determining gaps in the research.

The evolution of security models in cloud services reflects progress in understanding and countering cyber threats. Early research, including the foundational work of Mell and Grance from the National Institute of Standards and Technology [14], defined the basic principles of cloud computing, including service delivery models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These studies highlighted critical security threats associated with each model and offered initial recommendations for their management and mitigation.

Over time, research shifted towards creating more complex and multi-layered security models that consider various technical and organisational aspects [15]. Authors such as P. Sharma [16] demonstrated the need for an integrated approach to security, emphasising that data protection in cloud systems must encompass all levels of architecture – from physical data storage to applications and network interfaces [17–21]. These works expanded the understanding of how security provision should permeate every aspect of cloud infrastructure, highlighting the importance of data encryption, identity and access management, and regular monitoring and security auditing.

Further analysis by A.B.M. Shawkat Ali [22] delved deeper into the study of multi-layered protection, examining complex challenges associated with ensuring privacy and security in cloud services [23–26]. The authors explored specific threats, such as the misuse of cloud resources, data leakage, and vulnerabilities in Application Programming Interfaces (APIs) [27–30], proposing strategies to mitigate these threats through sophisticated encryption systems, advanced authentication and authorisation protocols, and the implementation of Intrusion Detection and Prevention Systems [31–35].

These studies underscored that cloud services require flexible and adaptive security models capable of responding to new challenges in a constantly evolving cyber threat landscape. They also pointed to the necessity of continuously improving security policies and procedures to stay abreast of the latest technological

developments and methods of cyber-attacks. These findings emphasise the importance of an integrated and multi-faceted approach to security in cloud platforms, which remains relevant in current research and practical developments in cybersecurity.

Contemporary threats and protective mechanisms

In the modern world, where cloud computing has become the foundation for data storage and processing, the importance of reliable security mechanisms cannot be overstated. Security threats to data on cloud platforms are becoming more sophisticated, necessitating constant vigilance and adaptation of protective systems by organisations and security professionals to new challenges. This condition prompts researchers and engineers to actively seek new approaches and solutions for security in the cloud environment.

Complexity of cloud security threats

DDoS (Distributed Denial of Service) attacks, phishing, insider threats, data breaches, and API vulnerabilities pose a serious risk to the security of cloud platforms [36–40]. Complex attacks that combine multiple vectors are hazardous, complicating their detection and neutralisation. For example, phishing attacks aimed at compromising credentials can be part of a more extensive campaign to gain unauthorised access to cloud resources and data.

Development of protective mechanisms

Data encryption continues to be a fundamental element of information protection in the cloud [41–44]. The advancement of cryptographic methods, including public essential encryption techniques and cryptographic key management technologies, provides robust data protection at rest and in transit.

Identity and Access Management (IAM) has evolved to include more complex management systems, such as multi-factor authentication and access management based on policies and roles. These mechanisms help minimise the risk of unauthorised access, ensuring that only authorised users have access to critical data and resources.

Intrusion Detection and Prevention Systems are becoming more intelligent. They incorporate machine learning algorithms to analyse traffic and detect anomalies in behaviour that may indicate a cyber attack. It allows for detecting known types of attacks and adaptation to new, previously unknown threats.

Innovations in cloud security

Applying Artificial Intelligence (AI) and Machine Learning (ML) in security opens new possibilities for protecting cloud platforms [45–48]. These technologies can significantly improve the ability to detect complex and disguised threats, offering automated solutions for their prevention. AI and ML can analyse large volumes of security data in real-time, identify hidden attack patterns, and predict potential threats before they cause harm.

Blockchain technologies are also interested in enhancing cloud services security, especially in terms of ensuring data integrity and secure identification [49–52]. Blockchain can offer solutions for protecting against data tampering and enhancing trust among participants in cloud services.

Methods

Developing an approach to comparing security models in cloud platforms requires meticulous planning and clear understanding of the research objectives. This methodology aims to analyse and compare various security models implemented by leading cloud platforms to identify their strengths and weaknesses and their effectiveness in protecting data and resources. To achieve this goal, a comprehensive approach that includes the following stages is proposed:

1. *Defining evaluation criteria*

The first step involves developing a system of criteria, by which the security models will be assessed. These criteria should cover key security aspects, such as data encryption, identity and access management, incident response, security monitoring and auditing, and compliance with regulatory requirements and standards. Each criterion must be clearly defined and measurable to ensure the objectivity and reproducibility of the comparison results.

2. *Selection of cloud platforms for analysis*

This stage entails selecting the cloud platforms to be included in the study. The selection is based on market share, innovative security approaches, and information availability about their security models. For a comprehensive analysis, choosing platforms representing different service models (IaaS, PaaS, SaaS) is recommended.

3. *Data collection*

Collecting data about the security models of each selected platform involves analysing official documents, technical specifications, security reports, and independent research. This stage requires careful attention to information sources to ensure the relevance and reliability of the collected data.

4. *Analysis and comparison*

Based on the collected data, each security model is analysed using the defined evaluation criteria. The analysis should reveal, which security mechanisms and approaches are used in each platform, and assess their effectiveness. Comparing the security models will highlight their strengths and weaknesses and identify best practices.

5. *Application of quantitative and qualitative evaluation methods*

Both qualitative and quantitative evaluation methods are applied to ensure the investigation objectivity.

Qualitative analysis allows for a deeper understanding of each security model context and characteristics, while quantitative methods, including rating systems and comparative tables, provide a clear visualisation of the differences and similarities between models.

6. *Conclusions and recommendations*

Based on the analysis and comparison, conclusions are drawn regarding, which security models are most effective in various contexts. Recommendations are also offered for cloud service developers and users of cloud platforms on selecting and optimising security models.

Criteria of security models

Developing and applying evaluation criteria and analysis of security models in cloud platforms is a crucial aspect of the research methodology. Clearly defined criteria allow for systematically comparing different approaches to ensuring security, identifying their advantages and disadvantages, and determining the most effective solutions. The developed criteria, their rationale, and the methodology for analysis are given below.

Data protection complexity

Criterion description: evaluates how comprehensively and multi-dimensionally the security model ensures data protection at all stages of its lifecycle: during creation, transmission, storage, and destruction.

Analysis methodology: the presence and effectiveness of cryptographic encryption mechanisms, data integrity measures, and secure data deletion methods are analysed.

Access and identity management

Criterion description: assesses the mechanisms for managing access to resources and data, including authentication, authorisation, user and system access logging, and control.

Analysis methodology: we examine the application of role-based policies, multi-factor authentication, privileged access management, and user action auditing capabilities.

Incident response and risk management

Criterion description: evaluates a cloud platform readiness for threat detection, response, and recovery after security incidents, as well as the ability to analyse and manage risks.

Analysis methodology: the paper analyses procedures for threat detection, incident response, system recovery after attacks, and risk assessment and management practices.

Compliance with regulatory requirements and standards

Criterion description: evaluates how the security model complies with international and national security standards and data protection legislation requirements.

Analysis methodology: we investigate the security model compliance with standards such as ISO/IEC 27001, GDPR, and HIPAA and the presence of compliance certificates and security reports.

Transparency and reporting

Criterion description: assesses the level of transparency of security practices and reporting capabilities for cloud platform users.

Analysis methodology: the availability and accessibility of security documentation, audit reports, and user tools and reports that allow monitoring of security events are considered.

Innovation and adaptability

Criterion description: evaluates the security model ability to adapt to new threats and integrate modern technological solutions, such as AI (Artificial Intelligence), ML (Machine Learning), and blockchain, to enhance security levels.

Analysis methodology: the application of advanced security technologies, the flexibility of the security architecture for innovation integration, and the system ability to learn and adapt to new threats are analysed.

Applying the developed criteria requires a systematic approach, including data collection and analysis and qualitative and quantitative evaluation of each security model. It implies using various research methods, including comparative analysis, expert evaluations, and case studies. The evaluation should be conducted objectively, considering each model strengths and weaknesses.

Criteria for selecting platforms for analysis

The platforms were chosen based on their market share, indicating their influence and significance in the cloud computing industry. Innovative security approaches, such as using AI for threat detection, data encryption, and identity management, were key selection factors. The availability of information about security measures was also a crucial criterion, allowing for a thorough and objective analysis of each platform.

This selection of platforms provides a broad overview of modern approaches to ensuring security in cloud services, covering common and unique protection strategies employed by leading providers.

Cloud platforms for analysis

For the analysis and comparison of security models, the following cloud platforms were selected: each holds a significant share in the cloud services market, demonstrates innovative approaches to security, and has sufficient information about its security measures.

1. Amazon Web Services (AWS)

AWS is a leader in the cloud computing market, offering a wide range of infrastructure services, from web hosting to high-performance computing. AWS

provides deep integration of security measures, including AWS IAM for access management, Amazon CloudWatch for monitoring, and Amazon Inspector for application security analysis. The company also actively utilises ML and AI to enhance the efficiency of its security systems [53–60].

2. Microsoft Azure

Azure offers an extensive set of cloud services supporting both Windows and Linux. The platform focuses on identity and access management with Azure Active Directory and offers data and application-level security tools, including Azure Security Center for centralised security management. Azure also emphasises the importance of compliance, providing extensive capabilities to adhere to international security standards [53, 55, 57, 58, 61].

3. Google Cloud Platform (GCP)

GCP stands out among other cloud platforms with its innovative security approaches, including using AI and ML for threat detection and data analysis. Google Cloud provides extensive capabilities for data encryption at rest and in transit, as well as identity and access management tools, including Cloud IAM. GCP also focuses on transparency and reporting, offering detailed security and compliance reports [53, 55, 58–61].

4. IBM Cloud

IBM Cloud offers a comprehensive set of cloud services with an emphasis on AI, ML, and cybersecurity. IBM Cloud security highlights the importance of comprehensive protection through data encryption, access and identity management, and real-time threat detection and prevention tools. IBM Cloud possesses powerful risk analysis and management capabilities and strictly adheres to international standards and regulatory requirements in data security [61–64].

5. Oracle Cloud

Oracle Cloud focuses on database and application security, offering solutions to protect critical corporate information. The platform includes powerful tools for data encryption, access management, security monitoring, and specialised tools for securing Oracle environments [65–69]. Oracle Cloud also provides detailed security configurations to meet the requirements of specific industries and regions.

Data security features of selected platforms

Ensuring data security is a paramount task for cloud platforms. Let us examine the features of each selected platform in the context of data security.

AWS offers extensive security tools and services focused on protecting client data. AWS security key aspects include data encryption at rest and in transit. AWS Key Management Service allows customers to create and manage encryption keys to protect data. AWS also provides multi-layered network protection capabilities, including setting up secure VPN connections and using Amazon CloudFront for secure data delivery [53–56, 58, 60, 70, 71]. Furthermore, AWS IAM enables fine-tuning access policies to resources and services, strengthening identity and access management.

MS Azure emphasizes the integration of its security services with the overall Microsoft security infrastructure, offering solutions such as Azure Active Directory for identity and access management. Azure Security Center provides a centralized view of the security state of cloud resources, offering recommendations for data protection enhancement [53, 55, 57, 58, 61, 72]. Azure employs both built-in encryption mechanisms for data storage and capabilities for client data encryption using their keys. Azure also supports a wide range of security standards and certifications, making it a suitable choice for enterprises operating in regulated industries.

GCP stands out with its approach to security, which is deeply integrated with its services and infrastructure. A key feature is the automatic encryption of all data at rest without needing special configurations from the client [53, 55, 58–61, 73]. GCP offers a unique tool, the Cloud Security Command Center, which provides a comprehensive view of the security state of cloud assets, allowing for the identification of vulnerabilities and unauthorized changes. GCP also actively uses ML to improve threat detection and anomalies in user and system behaviour.

IBM Cloud focuses on enterprise security, offering solutions specialized for industries with high data protection requirements, such as finance and healthcare. IBM Cloud provides extensive data encryption capabilities, including key management with IBM Key Protect [61–64, 74]. IBM Cloud is also notable for its approach to confidential computing, offering technologies that allow processing sensitive data in an encrypted form. Identification and access systems on IBM Cloud allow creating complex access management policies that integrate with corporate identity management systems.

Oracle Cloud emphasizes database protection, a key direction of its cloud strategy. Oracle offers advanced data encryption capabilities at the database level and for applications running in the cloud. Oracle Data Safe is a comprehensive data security service offering vulnerability assessment, data masking, and user activity monitoring features [65–69, 75]. Oracle Cloud provides powerful access and identity management tools, including multi-factor authentication and network segmentation, to ensure secure resource access.

Each platform presents a unique set of capabilities and approaches to data security, reflecting their individual strategies and target markets. Collectively, they illustrate the broad spectrum of modern technologies and practices in cloud security.

Specific security measures and technologies used in each cloud platform

Each cloud platform employs specific security measures and technologies to protect its clients' data. Here is a detailed overview of the technologies and security measures used by AWS(Amazon Web Services), Microsoft Azure, GCP (Google Cloud Platform), IBM Cloud, and Oracle Cloud.

Amazon Web Services [76]:

- *AWS IAM* allows for managing access to AWS resources by fine-tuning access policies for users and groups;
- *Amazon Cognito* simplifies authentication, authorization, and user management for web and mobile applications;
- *AWS Key Management Service* – centralized encryption key management that aids in creating and controlling keys used for data encryption;
- *Amazon GuardDuty* – threat detection service that monitors suspicious activity and unauthorized behavior;
- *AWS Shield* – DDoS protection service that automatically protects against the most common attacks.

Microsoft Azure [77]:

- *Azure Active Directory (AD)* is an identity and access service offering a suite of features for managing users and groups;
- *Azure Policy* helps meet corporate standards and service requirements for cloud resources;
- *Azure Security Center* provides unified security management and advanced threat protection for hybrid cloud environments;
- *Azure Information Protection* protects data regardless of where it resides, in the cloud or user devices;
- *Azure Advanced Threat Protection (ATP)* offers detection and response to advanced threats targeting corporate networks.

Google Cloud Platform [78]:

- *Cloud IAM* manages access to GCP resources with granularity down to individual resources;
- *Cloud Security Scanner* – automated web application scanner for finding vulnerabilities in applications hosted on GCP;
- *Data Loss Prevention API* helps discover and mask confidential information in data stored in GCP;
- *Google Cloud Armor* – service protecting against DDoS attacks and security threats for web applications and services;
- *Titan Security Key* – physical device for two-factor authentication, enhancing the protection of accounts.

IBM Cloud [79]:

- *IBM Cloud IAM* (Identity and Access Management) manages users and their access to IBM Cloud resources;
- *IBM Data Shield* offers data protection using confidential computing technology, allowing the processing and analysis of encrypted data;
- *IBM Hyper Protect Crypto Services* provides secure storage and management of cryptographic keys;
- *IBM Cloud Security Advisor* – centralized threat, vulnerability, and incident management dashboard;
- *IBM QRadar on Cloud* – Security Information and Event Management solution that helps detect anomalies and potential threats.

Oracle Cloud [80]:

- *Oracle Identity Cloud Service* provides access and identity management, offering powerful tools for managing users and their privileges;
- *Oracle Data Safe* – service that assists clients in discovering sensitive data, assessing database vulnerabilities, masking sensitive data, and monitoring database activity;
- *Oracle Cloud Infrastructure (OCI) Vault* manages encryption keys and secrets needed for data protection and resource access;
- *Oracle Advanced Security* offers transparent database and multi-layered data encryption, ensuring comprehensive data protection at all lifecycle stages;
- *Oracle Configuration and Compliance* – service to monitor and ensure cloud infrastructure configurations comply with security standards and regulatory requirements.

These specific security measures and technologies reflect the wide range of cloud data protection tools. Each platform develops solutions to satisfy its clients' security needs while showcasing unique innovations and approaches in cybersecurity.

Overview of known security breaches in reviewed cloud platforms

The history of cloud platforms has witnessed security breaches that serve as important lessons for improving data and system protection. Let’s examine some of these incidents involving AWS, Microsoft Azure, GCP, IBM Cloud, and Oracle Cloud.

AWS – notable incident related to AWS occurred in 2017 with Verizon. Data of almost 6 million Verizon customers became accessible due to incorrectly configured AWS S3 storage. The issue was that the storage access settings were changed to "public", allowing unauthorized data access. This case highlighted the importance of proper configuration and access management to cloud storages [81].

Microsoft Azure. In 2019, a vulnerable database server on Microsoft Azure was discovered, belonging to Microsoft and containing anonymized user data used for technical support. The data included personal information such as email addresses, IP addresses, and descriptions of equipment issues. Microsoft swiftly remedied the issue, emphasizing the importance of robust authentication mechanisms and data storage control [82].

GCP. In 2018, an incident with Google+, Google's social network, was uncovered on GCP, leading to potential exposure of private user profile information of up to 500,000 accounts. The problem was associated with the Google+ API, which allowed apps to access private profile information. Google shut down Google+ for consumers in response to this incident, underscoring the significance of rigorous API and data access control [83].

IBM Cloud. In 2020, a vulnerability in IBM Cloud was identified that could allow attackers to bypass authentication and gain access to IBM Cloud functions used for managing cloud services. IBM promptly addressed the vulnerability after its discovery. This case underscored the importance of regular audits and testing for vulnerabilities [84].

Oracle Cloud. In 2018, security researchers found several vulnerabilities in Oracle cloud infrastructure that could have allowed attackers to access clients' cloud resources. Oracle quickly responded to the reports and released the necessary patches. This incident highlights the necessity of continuous monitoring and updating security systems to protect against known and emerging threats [85, 86].

Analysis of the consequences of security breach incidents on various cloud platforms and the response measures taken by providers highlights the significance of vigilance in risk management and quick response to threats. Each of the discussed cases had unique circumstances that required specific actions by cloud providers to minimize damage and prevent similar incidents in the future.

Consequences and security response measures

AWS and the Verizon Incident. Consequences: The improperly configured S3 storage led to potential exposure of personal information of millions of Verizon customers. This incident underscored the importance of security competencies and correct cloud service configurations. Response Measures: AWS strengthened its information campaign on the importance of proper access policy settings for S3 storages, including the introduction of new visualization tools and automated access right checks.

Microsoft Azure and the Vulnerable Database Server. Consequences: The disclosure of anonymized user data pointed to deficiencies in authorization mechanisms and data storage control. Response Measures: Microsoft swiftly fixed the vulnerability and reviewed its security systems to detect and correct possible similar issues. The company also enhanced auditing processes and introduced additional data access controls.

GCP and the Google+ Incident. Consequences: The potential exposure of private user information on Google+ showed vulnerabilities in access control systems to APIs. Response Measures: Google decided to shut down Google+ for consumers and strengthened security checks for APIs, including stricter auditing and monitoring processes for developer API usage.

IBM Cloud and the Authentication Bypass Vulnerability. Consequences: The vulnerability in the authentication system exposed functionalities managing cloud services to risks. Response Measures: IBM swiftly mitigated the vulnerability and enhanced testing and auditing procedures for its security systems to detect such issues at earlier stages.

Oracle Cloud and Detected Vulnerabilities. Consequences: Vulnerabilities in Oracle Cloud infrastructure could have allowed attackers to access client data. Response Measures: Oracle quickly released patches to fix the vulnerabilities and enhanced its threat monitoring and detection systems. The company also stepped up efforts to inform clients about best security practices and configuration management.

The incidents that occurred on the AWS, Microsoft Azure, GCP, IBM Cloud, and Oracle Cloud platforms highlight the importance of a comprehensive approach to security, encompassing not just technological solutions but also risk management processes, staff training, and development of a security culture at all organizational levels. The response measures taken by the companies were aimed not only at addressing specific vulnerabilities, but also at enhancing the overall security level and resilience of the infrastructure against future threats.

Analysis and comparison of security models based on selected criteria

The comparative analysis of security models of five leading cloud platforms – AWS, Microsoft Azure, GCP, IBM Cloud, and Oracle Cloud – is conducted based on previously defined criteria: data protection complexity, access and identity management, incident response and risk management, compliance with regulatory requirements and standards, transparency and reporting, and innovation and adaptability.

Data protection complexity:

- AWS offers a broad spectrum of encryption tools and ensures high data protection at all stages. However, the complexity of configuration might be a barrier for some users.
- Azure possesses powerful encryption capabilities and integrates with other Microsoft products for comprehensive security. However, its dependence on the Microsoft ecosystem can lead to potential weaknesses.
- GCP automatically encrypts all data at rest, simplifying data protection management, but this may raise concerns about Google access to encryption keys.
- IBM Cloud focuses strongly on data protection for enterprise clients with high-security requirements,

though its services might be less flexible for small and medium businesses.
- Oracle Cloud stands out with its database protection solutions, making it an ideal choice for organizations, which databases are critical assets. However, the complexity and cost of solutions might be prohibitive for some users [76–80].

Access and identity management:
- AWS IAM allows detailed access policy settings, but its complexity can challenge new users.
- Azure Active Directory offers robust identity management capabilities, but its effectiveness is maximized compared to other Microsoft products.
- GCP provides flexible access and identity management, including integration with external accounts, which can be especially valuable for hybrid cloud environments.
- IBM Cloud offers advanced IAM features geared towards corporate users. These features provide a high level of protection but potentially limit flexibility in some scenarios.
- Oracle Cloud integrates with existing corporate identity systems, providing secure and convenient access management, though integration with non-Oracle systems may be complex [76–80].

Incident response and risk management:
- AWS and Azure offer extensive incident response and risk management tools, including automated mechanisms for threat tracking and attack prevention. However, they require significant effort for configuration and monitoring.
- GCP actively uses ML for threat detection and offers user-friendly tools for risk management, which can be particularly useful for companies without a large IT security department.
- IBM Cloud and Oracle Cloud offer specialized incident response and risk management solutions, aimed at large corporations with high security and regulatory compliance requirements [76–80].

Compliance with regulatory requirements and standards:

All platforms offer robust tools and services to comply with international standards and regulatory requirements, such as GDPR, HIPAA, and PCI DSS. However, the degree of integration and ease of use varies, with AWS and Azure, providing the most developed and accessible resources for users to achieve and maintain compliance [76–80].

Transparency and reporting:
- AWS and Azure provide extensive capabilities for security monitoring and reporting, though the complexity of their interfaces may prevent their effective use.
- GCP stands out with its intuitive tools for visualizing and analyzing security data, simplifying incident tracking and response.
- IBM Cloud and Oracle Cloud offer advanced reporting tools for corporate clients' needs, which may be less convenient for small and medium businesses [76–80].

Innovation and adaptability:
- AWS and GCP are notable for their innovative approaches to security. They actively incorporate the latest technologies, such as ML and AI, to improve threat detection and adapt to new challenges.
- Azure continues to develop its security services, closely integrating them with other Microsoft products, providing versatility and depth of protection.
- IBM Cloud and Oracle Cloud focus on specialized solutions for industry and corporate clients, ensuring a high level of protection but may limit their flexibility and innovation for a broader range of users [76–80].

Advantages and disadvantages of security systems in leading cloud platforms based on previously defined criteria

Amazon Web Services (AWS)

Advantages:
- Broad range of security tools: AWS offers an extensive array of services and tools for data, network, and identity protection, making it a powerful platform for security at all levels.
- Deep integration with ML and AI: AWS uses advanced technologies for threat detection and data analysis, enhancing the effectiveness of its security mechanisms.
- Scalability: security in AWS can scale alongside a business growing needs without compromising protection quality.

Disadvantages:
- Complexity in management: various tools and services can complicate security management, especially for new users.
- Dependence on proper configuration: many security incidents on AWS are linked to user misconfiguration, highlighting the need for in-depth knowledge for practical use.

Microsoft Azure

Advantages:
- Integration with Microsoft ecosystem: Azure offers tight integration with other Microsoft products and services, facilitating security management in complex environments.
- Advanced IAM capabilities: Azure Active Directory provides robust identity and access management functions, ensuring deep resource control.
- Strong compliance support: Azure actively works towards meeting international and industry-specific security standards, appealing to large businesses and regulated sectors.

Disadvantages:

- Dependence on Microsoft ecosystem: maximum efficiency is achieved when combined with other Microsoft products, which may limit options for companies with diverse IT landscapes.
- Complexity in configuration and management: some users report high complexity in setting up and managing security in Azure.

Google Cloud Platform (GCP)

Advantages:

- Security innovations: GCP actively implements the latest technologies, including ML, for enhanced security, positioning it as a leader in innovations.
- Automatic data encryption: all data is automatically encrypted in GCP, reducing the risk of information leakage.
- Ease of use: GCP offers user-friendly security management tools, simplifying smaller teams tasks.

Disadvantages:

- Lower market penetration: despite its innovations, GCP has a smaller market share compared to AWS and Azure, which may affect the availability of integrations and third-party solutions.
- Limited information on some security aspects: users may encounter a lack of detail in official documentation on specific security issues.

IBM Cloud and Oracle Cloud

Both platforms showcase strong capabilities in providing security for enterprise clients, particularly in sectors with high data protection requirements. They offer advanced solutions for encryption, identity management, and compliance with standards. However, like other platforms, they may face challenges in management complexity and integration into existing infrastructure, especially in mixed and diverse IT environments.

Common disadvantages of IBM Cloud and Oracle Cloud:

- High cost and complexity for SMEs: products from both providers can be expensive and complex to configure and manage for small and medium enterprises.
- Focus on corporate clients: while this may be an advantage for large businesses, smaller companies might find that the products and services do not fully meet their needs.

Evaluating the importance of chosen criteria for analyzing cloud platforms

The significance of the selected security evaluation criteria for cloud platforms can vary depending on the specifics of the business, security requirements, and organizational priorities. Nevertheless, the author offers a generalized assessment based on commonly accepted cloud security and risk management practices.

- *Data protection complexity*: encryption, key management, and data protection at rest and in transit – 20%. Data is the most valuable asset for most organizations, and its protection must be a top priority. This criterion receives a high percentage because the absence of proper data protection can lead to significant financial losses and reputation damage.
- *Access and identity management*: identity management, multi-factor authentication, privilege minimization – 20%. Controlling who can access data and resources is critical for ensuring security. This criterion covers everything from user authentication and authorization to privilege management and access policies. Security breaches often occur due to vulnerabilities in access management systems, justifying the high importance of this criterion.
- *Incident response and risk management*: incident readiness, risk analysis, and recovery plans after failures – 15%. The ability to quickly respond to security incidents and effectively manage risks helps minimize potential damage from attacks and breaches. This criterion receives a slightly lower percentage because, ideally, security systems should prevent incidents before they occur, but realism requires preparedness for inevitable incidents.
- *Compliance with regulatory requirements and standards*: compliance with GDPR, HIPAA, PCI DSS, and other standards and regulations – 15%. This is mandatory for many organizations and serves as proof of commitment to best security practices. This aspect is critical for maintaining customer and partner trust and avoiding legal consequences and fines.
- *Transparency and reporting*: availability of security reports, audits, and monitoring – 10%. Transparency in security operations and reporting availability are essential for stakeholder trust and internal risk management. This criterion receives a lower percentage because while it is important for overall security management, its impact on direct threat prevention and data protection may be less evident than that of other criteria.
- *Innovation and adaptability*: implementation of the latest technologies and approaches, flexibility, and the ability to adapt to new threats – 20%. Adapting to new threats and integrating the latest technologies into cloud platform protection is crucial in the dynamic world of cybersecurity. Innovations enhance the efficiency of security systems and provide a strategic advantage in protection against competitors. This criterion receives a high percentage, emphasizing the importance of continuous development and improvement of security measures in response to current and future threats.

This distribution reflects a balanced approach to assessing the security of cloud platforms, highlighting the importance of threat prevention and data protection, access management, incident response, compliance, transparency, and innovation.

Evaluating each security criterion for platforms AWS, Microsoft Azure, GCP, IBM Cloud, and Oracle Cloud based on the information provided in previous sections and the established significance distribution of criteria is a complex task. We will use a scale from 1 to 10, where 1 signifies low compliance with security criteria, and 10 signifies high. These ratings are approximate and based on publicly available information and security discussions. Fig. 1–6 present the platform evaluation results for each criterion in diagrams.

Fig. 1. *Data protection complexity scores*
Рис. 1. *Оценка сложности защиты данных*

AWS and GCP stand out with their comprehensive approaches to data protection, including broad encryption capabilities and key management. Azure, IBM Cloud, and Oracle Cloud also offer robust solutions but with some caveats regarding integration and ease of use.

Fig. 2. *Access management and identification*
Рис. 2. *Управление доступом и идентификация*

AWS and Azure offer advanced access management and identification tools, including powerful IAM capabilities. GCP and IBM Cloud also perform well in this task but with some limitations. Oracle Cloud lags in this aspect due to less flexibility and integration.

Fig. 3. *Incident response and risk management*
Рис. 3. *Реагирование на инциденты и управление рисками*

AWS, Azure, and IBM Cloud provide strong incident response and risk management tools. GCP and Oracle Cloud possess commendable capabilities but with some restrictions compared to the leaders.

Fig. 4. *Regulatory compliance and standards*
Рис. 4. *Соответствие нормативным требованиям и стандартам*

AWS and Azure stand out for ensuring compliance with international and industry-specific security standards. GCP, IBM Cloud, and Oracle Cloud also offer suitable solutions in this direction, but with a slight lag behind the leaders.

Fig. 5. *Transparency and reporting*
Рис. 5. *Прозрачность и отчетность*

GCP distinguishes itself with its transparency and reporting capabilities, especially using AI for security data analysis. AWS and Azure also provide robust tools in this area. IBM Cloud and Oracle Cloud have certain shortcomings in terms of monitoring and reporting convenience.

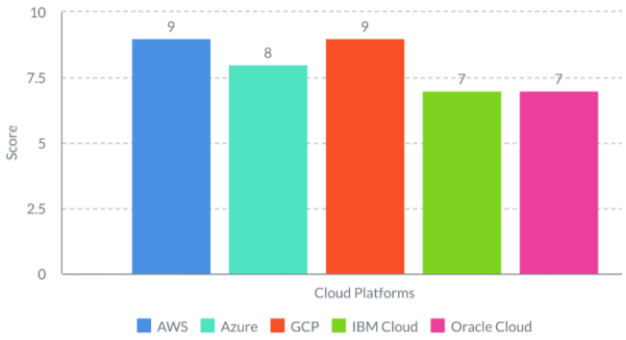

Fig. 6. *Innovation and adaptability*
Рис. 6. *Инновации и адаптивность*

AWS and GCP lead innovation and adaptability, incorporating the latest technologies and approaches into their platforms. Azure follows them with a slight lag. IBM Cloud and Oracle Cloud offer innovative solutions at a slower pace and scale.

These ratings reflect each cloud platform current state and development directions regarding security. It is important to note that the ratings are based on a generalised analysis and may vary depending on specific usage scenarios and organisational needs.

The normalisation and summarisation of the security criteria ratings for cloud platforms consisted of several key steps:

Criteria identification and weight assignment: Initially, the security evaluation criteria for cloud platforms were defined, such as data protection complexity, access management and identification, incident response and risk management, compliance with regulatory requirements and standards, transparency and reporting, and innovation and adaptability. Each criterion was assigned a specific weight in percentages, reflecting its significance in the overall security assessment.

Platform evaluation by criteria: Subsequently, each cloud platform (AWS, Azure, GCP, IBM Cloud, Oracle Cloud) was rated for each criterion on a scale from 1 to 10, where 1 signifies low compliance with security requirements, and 10 indicates high compliance.

Score normalisation: For each platform, the scores for the criteria were multiplied by the criterion weight (a percentage value converted into a fraction) to obtain normalised values. This allowed considering not just the platforms absolute ratings for each criterion but also the importance of these criteria within the overall security context.

Results summation: Finally, the normalised values for all criteria were summed up for each cloud platform to obtain a total score that reflects a comprehensive assessment of the cloud platform security, considering the importance of each criterion.

This process ensured a balanced and comprehensive evaluation of cloud platform security, taking into account each platform strengths and potential vulnerabilities in the context of the presented criteria. The results of normalisation and summation provide a quantitative expression of the security level, facilitating a more informed choice of cloud platform from a data security perspective.

After normalising the ratings, taking into account the significance of each criterion, we get the following results (Fig. 7):

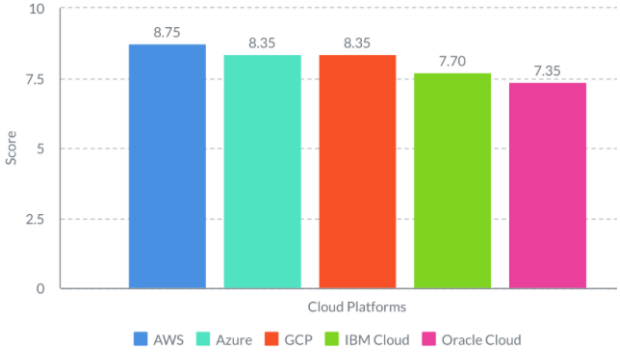

Fig. 7. *Summary ranking of cloud platforms based on aggregate features*
Рис. 7. *Сводный рейтинг облачных платформ на основе совокупных характеристик*

These ratings provide a comprehensive evaluation of cloud platform security, considering the importance of each aspect discussed. AWS highest overall score indicates its leading position in comprehensive data security. Azure and GCP show nearly identical outcomes, occupying strong positions with a slight lag behind AWS. IBM Cloud and Oracle Cloud have lower ratings, indicating limitations in their current security models compared to the leaders.

Conclusion

During our investigation, we detailedly analysed the security models of the five largest cloud platforms: AWS, Microsoft Azure, GCP, IBM Cloud, and Oracle Cloud. Focus was given to data protection complexity, access management and identification, the ability to respond to incidents and manage risks, compliance with regulatory requirements and standards, transparency and reporting, and innovation and adaptability.

The research shows that leading cloud platforms offer a high level of security, actively utilising advanced encryption technologies and effective access manage-

ment systems. Particular attention is paid to using AI and ML to enhance the efficiency of threat detection and prevention.

Innovative approaches, including confidential computing and application of blockchain technologies, are becoming increasingly common, allowing cloud platforms not only effectively protecting data and systems but also ensuring their resilience to future threats. It is important to note that all platforms make significant efforts to comply with international and industry security standards, which is critical for maintaining user trust and regulatory compliance.

Based on the analysis, the cloud computing industry demonstrates a high degree of commitment to security issues, actively investing in developing and implementing advanced technologies and practices. This lays the foundation for further development and strengthening of cloud platform security in the future, which is a key factor for maintaining and expanding its use across various business and technology sectors.

Assessing the significance of security evaluation criteria for cloud platforms is a multifaceted process that invariably depends on each organisation unique needs, goals, and structural characteristics. The specifics of the business determine, which data and applications are critical and, therefore, which aspects of security require the most attention. For example, companies operating in the financial sector or healthcare may pay particular attention to compliance with regulatory requirements and standards, whereas for technology startups, innovation and security adaptability to new threats may be more crucial.

Security requirements are formed based on risk and threat analysis for the specific business. This means that organisations highly dependent on cloud technologies may focus on access management and identification to minimise the risks of unauthorised access to data and resources. In this process, transparency and reporting may be rated higher in conditions where the need for transparent data management and accountability to regulatory bodies becomes a key factor for maintaining customer trust and legislative compliance.

Furthermore, organisation security priorities may change as technologies evolve, security threat landscapes change, and business strategies are modified. In this context, a cloud platform ability to innovate and adapt to new conditions becomes a critical criterion influencing the choice of cloud service provider.

In conclusion, assessing the significance of cloud platform security criteria in percentage terms reflects a comprehensive approach to evaluating security levels tailored to the organisation specific needs and goals. It underscores the need for a deep understanding of one's own security requirements and careful consideration in choosing a cloud provider, whose capabilities and security policies best meet these requirements.

Discussions

In cloud data security, new trends and technologies constantly emerge in response to the evolution of cyber threats and changing information protection requirements. Modern approaches and innovations aim to enhance data security levels in cloud environments, considering the specificities of cloud architectures and integrating them with existing security systems. Let us explore some of this field most promising technologies and approaches.

Confidential computing

Confidential computing is a technology that enables the processing and analysis of encrypted data without decryption. It provides a new level of data protection, allowing users and companies to safely share information and use cloud services for processing sensitive data without worrying about leaks or unauthorised access. The application of confidential computing extends from financial services to healthcare, where the demands for confidentiality and data protection are exceptionally high [87].

Blockchain and distributed ledgers

Blockchain and distributed ledger technologies enhance cloud data security by creating reliable and immutable systems for data and transaction logging. Blockchain can be used to protect supply chains, digital identities, and smart contracts and to ensure secure data exchange among participants in a cloud infrastructure. The immutability and transparency of blockchain provide additional trust and security in cloud applications [88].

Artificial Intelligence and Machine Learning

Using AI and ML in cloud data security allows creating systems capable of adapting to new threats and effectively detecting anomalies in system and user behaviour. ML algorithms analyse vast data on network traffic and user actions, identifying potential threats and unusual patterns, significantly increasing the speed and accuracy of security incident responses [89].

Managed identity and access services

Managed identity and access services provide centralised management of digital identities and access policies in cloud environments. Integration with cloud platforms automates authentication and authorisation, ensuring high application and data protection. Advanced identity management features include multifactor authentication, single sign-on, and privileged access management [90].

API security

API security issues become critically important with the widespread use of APIs for integrating cloud services and applications. API protection mechanisms,

including traffic encryption, authentication and authorisation of requests, rate limiting, and monitoring, help prevent attacks targeting application interface vulnerabilities [91].

Automated configuration management

Automated configuration management ensures compliance with security standards and company policies in cloud infrastructure. Tools such as Terraform and Ansible automatically deploy and configure cloud resources according to predefined security templates, reducing the risk of human error and enhancing data protection [92].

These new technologies and approaches to cloud data security represent just a part of modern organisations wide range of tools and methods for protecting their digital assets in cloud environments.

As cloud technologies continue to evolve, offering new opportunities for scaling, flexibility, and innovation, the complexity of ensuring data security also increases. In this context, cloud data security models also undergo significant changes, adapting to new threats and technological trends. Let us consider the possible future developments in these models:

Autonomous security using AI and ML

AI and ML advancements foresee a future where security systems can independently detect, analyse, and respond to threats without constant human intervention. These systems will be able to adapt to the changing threat landscape, automatically adjusting protective mechanisms and security policies [93].

Enhanced data privacy protection through confidential computing

Confidential computing technologies, which allow processing encrypted data without decryption, will evolve and find increasingly widespread applications. It will enable organisations to use cloud services to process sensitive data while ensuring high confidentiality and regulatory compliance [94].

Development of quantum cryptography

With the advancement of quantum technologies, there is potential for creating encryption systems that are resistant to attacks using quantum computers. Quantum cryptography could become a key element in protecting data on cloud platforms, offering methods of information transfer that cannot be intercepted or decrypted without knowledge of data integrity breaches [95].

Distributed security and blockchain

Blockchain and distributed ledger technologies will be integrated into cloud platforms to create decentralised security systems that provide reliable identity management, authentication, and authorisation. Blockchain can be used to create tamper-proof digital signatures, transaction logging, and protection against data manipulation [96].

Chip-level and hardware security

Security at the hardware level will become even more critical as attacks become more sophisticated. Developing and implementing specialised chips and hardware devices for cloud data security, including secure boot processes and processor-level encryption, will play a key role in protecting cloud resources [97].

Expanded capabilities for identity and access management

The need for more granular access management grows as the number of cloud services and applications increases. Future security models will offer even more advanced identity and access management solutions, including biometric authentication, identity lifecycle management, and integration with corporate access management systems [98].

These directions in cloud data security development reflect the general trend towards creating more autonomous, adaptive, and threat-resilient systems. Implementing new technologies and approaches requires a careful balance between innovation and proven security methods, as well as continuous collaboration between cloud service providers, security developers, and users of cloud platforms.

REFERENCES

1. Zscaler, Inc. 2021 Gartner Hype Cycle for Cloud Security. *Zscaler, Inc*. Available at: https://info.zscaler.com/resources-report-2021-gartner-hype-cycle-for-cloud-security (accessed: 13 January 2024).
2. Trend Micro Incorporated. Trend Micro Cloud App Security Threat Report 2021. *Trend Micro Incorporated*. Available at: https://www.trendmicro.com/en_gb/business.html (accessed: 13 January 2024).
3. Zhang G., MacCarthy B.L., Ivanov D. The cloud, platforms, and digital twins – enablers of the digital supply chain. *The Digital Supply Chain*. Elsevier, 2022. pp. 77–91.
4. Atieh A.T. The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges. *ResearchBerg Review of Science and Technology*, 2021, vol. 1, no. 1, pp. 1–15.
5. Tissir N., El Kafhali S., Aboutabit N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, 2021, vol. 7, no. 2, pp. 69–84.
6. Akhtar N. A comprehensive overview of privacy and data security for cloud storage. *International Journal of Scientific Research in Science Engineering and Technology*, 2021, vol. 8, pp. 112–152.
7. Oladoyinbo T.O. Evaluating and establishing baseline security requirements in cloud computing: an enterprise risk management approach. *Asian Journal of Economics, Business and Accounting*, 2023, vol. 23, no. 21, pp. 222–231.
8. Kamiya S. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 2021, vol. 139, no. 3, pp. 719–749.

9. Jangjou M., Sohrabi M.K. A comprehensive survey on security challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering*, 2022, vol. 29, no. 6, pp. 3587–3608.
10. Thapa C., Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, 2021, vol. 129, pp. 104130.
11. Alouffi B. A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, 2021, vol. 9, pp. 57792–57807.
12. Jain A.K., Gupta B.B. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, 2022, vol. 16, no. 4, pp. 527–565.
13. Kraus S. Digital transformation: an overview of the current state of the art of research. *Sage Open*, 2021, vol. 11, no. 3, pp. 21582440211047576.
14. Mell P., Grance T. The NIST definition of cloud computing, *National Institute of Standards and Technology//NIST Special Publication 800-145*, 2011.
15. Hong J.B., Kim D.S. Towards scalable security analysis using multi-layered security models. *Journal of Network and Computer Applications*, 2016, vol. 75, pp. 156–168.
16. Sharma P., Johari R., Sarma S.S. Integrated approach to prevent SQL injection attack and reflected cross site scripting attack. *International Journal of System Assurance Engineering and Management*, 2012, vol. 3, pp. 343–351.
17. King N.J., Raja V.T. Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, 2012, vol. 28, no. 3, pp. 308–319.
18. Gonzalez N. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 2012, vol. 1, pp. 1–18.
19. Martens B., Teuteberg F. Decision-making in cloud computing environments: a cost and risk based approach. *Information Systems Frontiers*, 2012, vol. 14, pp. 871–893.
20. Xu X. From cloud computing to cloud manufacturing. *Robotics and computer-integrated manufacturing*, 2012, vol. 28, no. 1, pp. 75–86.
21. Badger L., Grance T. Cloud computing synopsis and recommendations-recommendations of the national institute of standards and technology, *National Institute of Standards and Technology// NIST Special Publication*, 2012, pp. 800–146.
22. Habiba M., Islam M.R., Ali A.B.M.S. Access control management for cloud. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. Melbourne, VIC, Australia, 2013. pp. 485–492.
23. Kardas S. A new security and privacy framework for RFID in cloud computing. *2013 IEEE 5th international conference on cloud computing technology and science*, Bristol, UK, 2013. Vol. 1, pp. 171–176.
24. Kumar S. An approach of creating a private cloud for universities and security issues in private cloud. *International Journal of Advanced Computing*, 2013, vol. 36, no. 1, pp. 1134–1137.
25. Ali M., Miraz M.H. Cloud computing applications. *Proceedings of the International Conference on Cloud Computing and eGovernance*. UAE, 2013. Vol. 1, pp. 1–8.
26. Whitley E.A., Willcocks L.P., Venters W. Privacy & security in the Cloud. *Journal of International Technology and Information Management*, 2013, vol. 22, no. 3, pp. 75–92.
27. Lu Q. Cloud API issues: an empirical study and impact. *Proceedings of the 9th international ACM Sigsoft conference on Quality of software architectures*, Vancouver, Canada, 2013. pp. 23–32.
28. Silva L.A.B., Costa C., Oliveira J.L. A common API for delivering services over multi-vendor cloud resources. *Journal of Systems and Software*, 2013, vol. 86, no. 9, pp. 2309–2317.
29. Gracia-Tinedo R., Artigas M.S., Lopez P.G. Cloud-as-a-Gift: Effectively exploiting personal cloud free accounts via REST APIs. *2013 IEEE Sixth International Conference on Cloud Computing*, Santa Clara, CA, USA, 2013. pp. 621–628.
30. Cunha D., Neves P., Sousa P. A platform-as-a-service api aggregator. *Advances in Information Systems and Technologies*. Berlin Heidelberg, Springer, 2013. pp. 807–818.
31. Patel A. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*, 2013, vol. 36, no. 1, pp. 25–41.
32. Iqbal S. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, 2016, vol. 74, pp. 98–120.
33. Mehmood Y. Intrusion detection system in cloud computing: Challenges and opportunities. *2013 2nd national conference on information assurance (NCIA)*. Rawalpindi, Pakistan, 2013. pp. 59–66.
34. Radoglou-Grammatikis P.I., Sarigiannidis P.G. Securing the smart grid: a comprehensive compilation of intrusion detection and prevention systems. *Ieee Access*, 2019, vol. 7, pp. 46595–46620.
35. Baykara M., Das R. A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications*, 2018, vol. 41, pp. 103–116.
36. Al Nafea R., Almaiah M.A. Cyber security threats in cloud: Literature review. *2021 international conference on information technology (ICIT)*, Amman, Jordan, 2021. pp. 779–786.
37. Alenizi B.A., Humayun M., Jhanjhi N.Z. Security and privacy issues in cloud computing. *Journal of Physics: Conference Series. IOP Publishing*, 2021, vol. 1979, no. 1, pp. 012038.
38. Aslan Ö. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 2023, vol. 12, no. 6, pp. 1333.
39. Sasubilli M.K., Venkateswarlu R. Cloud computing security challenges, threats and vulnerabilities. *2021 6th international conference on inventive computation technologies (ICICT)*, Coimbatore, India, 2021. pp. 476–480.
40. Abdulsalam Y.S., Hedabou M. Security and privacy in cloud computing: technical review. *Future Internet*, 2021, vol. 14, no. 1, pp. 11.
41. Song H., Li J., Li H. A cloud secure storage mechanism based on data dispersion and encryption. *IEEE Access*, 2021, vol. 9, pp. 63745–63751.
42. El Kafhali S., El Mir I., Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, 2022, vol. 29, no. 1, pp. 223–246.

43. Gupta I. Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEE Access*, 2022, vol. 10, pp. 71247–71277.
44. Seth B. Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, 2022, vol. 33, no. 4, pp. e4108.
45. Nassif A.B. Machine learning for cloud security: a systematic review. IEEE Access, 2021, vol. 9, pp. 20717–20735.
46. Rath M., Satpathy J., Oreku G.S. Artificial intelligence and machine learning applications in cloud computing and Internet of Things. *Artificial intelligence to solve pervasive internet of things issues*. Academic Press, 2021. pp. 103–123.
47. Ahmed S. Artificial intelligence and machine learning for ensuring security in smart cities. *Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances*. Cham, Springer International Publishing, 2021. pp. 23–47.
48. Hernandez-Jaimes M.L. Artificial intelligence for IoMT security: a review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. *Internet of Things*, 2023. pp. 100887.
49. Habib G. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, 2022, vol. 14, no. 11, pp. 341.
50. Mustafa M. Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems. *Computational and mathematical methods in medicine*, 2022, vol. 2022, pp. 1–10.
51. Fatima N., Agarwal P., Sohail S.S. Security and privacy issues of blockchain technology in health care – a review. *ICT Analysis and Applications*, 2022, vol. 134, pp. 193–201.
52. Kollu P.K. Blockchain techniques for secure storage of data in cloud environment. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021, vol. 12, no. 11, pp. 1515–1522.
53. Gupta B., Mittal P., Mufti T. A review on amazon web service (aws), microsoft azure & google cloud platform (GCP) services. *Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020*, Jamia Hamdard, New Delhi, India, 27–28 February 2020. pp. 1–9.
54. Kewate N. A review on AWS-cloud computing technology. *International Journal for Research in Applied Science and Engineering Technology*, 2022, vol. 10, no. 1, pp. 258–263.
55. Yevge A. Review paper on cloud service provider – AWS, Azure, GCP, *EasyChair preprint*, 2022.
56. Naseer I. AWS cloud computing solutions: optimizing implementation for businesses. Statistics, computing and interdisciplinary research, 2023, vol. 5, no. 2, pp. 121–132.
57. Hassan M. Microsoft Azure's Leading Edge in Cloud Computing Services. *IUP Journal of Computer Sciences*, 2022, vol. 16, no. 2, pp. 46.
58. Boneder S. *Evaluation and comparison of the security offerings of the big three cloud service providers Amazon Web Services, Microsoft Azure and Google Cloud Platform*. Diss. Technische Hochschule Ingolstadt, 2023.
59. Dantas V. Architecting Google Cloud Solutions: learn to design robust and future-proof solutions with Google Cloud technologies. Birminham-Mumbai, Packt Publ. Ltd, 2021. 454 p.
60. Alluri G.T. *Performance Evaluation of Apache Cassandra using AWS (Amazon Web Services) and GCP (Google Cloud Platform)*. Diss. Blekinge, 2022.
61. Opara E., Wimmer H., Rebman C.M. Auto-ML cyber security data analysis using Google, Azure and IBM Cloud Platforms. *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET).* Prague, Czech Republic, 2022. pp. 1–10.
62. Panwar A. A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. *Computational Intelligence and Neuroscience*, 2022, vol. 2022, pp. 1–19.
63. Zulifqar I., Anayat S., Kharal I. A review of data security challenges and their solutions in cloud computing. *International Journal of Information Engineering & Electronic Business*, 2021, vol. 13, no. 3, pp. 30–38.
64. Fadhil I.S.M., Nizar N.B.M., Rostam R.J. Security and privacy issues in cloud computing. *TechRxiv*, 2023, pp. 1–9.
65. Sun R., Gregor S., Fielt E. Generativity and the paradox of stability and flexibility in a platform architecture: A case of the Oracle Cloud Platform. *Information & Management*, 2021, vol. 58, no. 8, pp. 103548.
66. Al Moaiad Y. Cloud service provider cost for online university: Amazon Web Services versus Oracle Cloud Infrastructure. *International Visual Informatics Conference*. Singapore, Springer Nature Singapore, 2023. pp. 302–313.
67. Kvet M. *Developing robust date and time oriented applications in Oracle Cloud: a comprehensive guide to efficient date and time management in Oracle Cloud*. Birmingham, Packt Publ. Ltd, 2023. 438 p.
68. Susanto A. Comparative analysis of key management service performance on AWS, Google Cloud, and Oracle Cloud with performance testing. *2023 11th International Conference on Cyber and IT Service Management (CITSM)*. Makassar, Indonesia, 2023. pp. 1–6.
69. Bell C. Oracle Cloud Infrastructure. *MySQL Database Service Revealed: Running MySQL as a Service in the Oracle Cloud Infrastructure*. Berkeley, CA, Apress, 2022. pp. 17–75.
70. Galiveeti S. Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. *Artificial intelligence and blockchain for future cybersecurity applications*. Cham, Springer International Publishing, 2021. pp. 329–360.
71. Mishra S. A survey on AWS cloud computing security challenges & solutions. *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*. Madurai, India, 2022. pp. 614–617.
72. Ahmad W. Cyber security in iot-based cloud computing: a comprehensive survey. *Electronics*, 2021, vol. 11, no. 1, pp. 16.
73. Roy A., Banerjee A., Bhardwaj N. A study on Google Cloud Platform (GCP) and its security. *Machine Learning Techniques and Analytics for Cloud Security*, 2021, pp. 313–338.
74. Mishra P., Pilli E.S., Joshi R.C. Cloud security: attacks, techniques, tools, and challenges. *Chapman and Hall/CRC*, 2021, 242 p.
75. Aylapuram S.S.C. Challenges of implementing Cloud Security System through Identity, Access & Risk Management [IARM] in a hybrid IT environment. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2022, vol. 13, no. 03, pp. 691–698.
76. AWS. Security, Identity, and Compliance. *AWS Documentation*. Available at: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-services.html (accessed: 15 January 2024).

77. *Microsoft. Azure Documentation*. URL: https://learn.microsoft.com/en-us/azure/?product=popular (accessed: 15 January 2024).
78. *Google Cloud. Security and Identity*. Available at: https://cloud.google.com/security/products/security-and-identity (accessed: 15 January 2024).
79. IBM. IBM Cloud Docs. *IBM Cloud*. Available at: https://cloud.ibm.com/docs (accessed: 15 January 2024).
80. Oracle. Cloud Security Services. *Oracle*. Available at: https://www.oracle.com/security/cloud-security/ (accessed: 15 January 2024).
81. Trend Micro. Verizon's Internal Data Exposed on Unprotected AWS Server. *Trendmicro*. Available at: https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/verizon-s-internal-data-exposed-on-unprotected-aws-server (accessed: 15 January 2024).
82. Dark reading. Microsoft Azure Cloud Vulnerability Exposed Thousands of Databases. *Dark Reading*. Available at: https://www.darkreading.com/cloud-security/microsoft-azure-cloud-vulnerability-exposed-thousands-of-databases (accessed: 15 January 2024).
83. The Verge. Google is shutting down Google+ for consumers following security lapse. *The Verge*. Available at: https://www.theverge.com/2018/10/8/17951890/google-plus-shut-down-security-api-change-gmail-android (accessed: 15 January 2024).
84. Security Week. Critical Remote Code Execution Vulnerabilities Patched in IBM WebSphere. *Security Week*. Available at: https://www.securityweek.com/critical-remote-code-execution-vulnerabilities-patched-ibm-websphere/ (accessed: 15 January 2024).
85. Oracle. Oracle Security Alert Advisory – CVE-2018-3110. *Oracle*. Available at: https://www.oracle.com/security-alerts/alert-cve-2018-3110.html (accessed: 15 January 2024).
86. Dark reading. Oracle Counters SQL – injection holes with update. *Dark Reading*. Available at: https://www.darkreading.com/cyber-risk/oracle-counters-sql-injection-holes-with-update (accessed: 15 January 2024).
87. Valadares D.C.G. Confidential computing in cloud/fog-based Internet of Things scenarios. *Internet of Things*, 2022, vol. 19, pp. 100543.
88. Neetha S.S. A survey paper on cloud security based on distributed ledgers of blockchain. *International Research Journal on Advanced Science Hub*, 2021, vol. 3, no. 3, pp. 38–42.
89. Lăzăroiu G. Artificial intelligence algorithms and cloud computing technologies in blockchain-based fintech management. *Oeconomia Copernicana*, 2023, vol 14, no. 3, pp. 707–730.
90. Farid F. A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. *Sensors*, 2021, vol. 21, no. 2, pp. 552.
91. Parast F.K. Cloud computing security: a survey of service-based models. *Computers & Security*, 2022, vol. 114, pp. 102580.
92. Gurbatov G. A comparison between Terraform and Ansible on their impact upon the lifecycle and security management for modifiable cloud infrastructures. *OpenStack*, 2022, pp. 51–131.
93. Kanimozhi V., Jacob T.P. Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express*, 2021, vol. 7, no. 3, pp. 366–370.
94. Pothireddy S. Data security in cloud environment by using hybrid encryption technique: a comprehensive study on enhancing confidentiality and reliability. *International Journal of Intelligent Engineering & Systems*, 2024, vol. 17, no. 2, pp. 159–173.
95. Ukwuoma H.C. Post-quantum cryptography-driven security framework for cloud computing. *Open Computer Science*, 2022, vol. 12, no. 1, pp. 142–153.
96. Li W. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, 2021, vol. 10, no. 1, pp. 35.
97. Nagata M., Miki T., Miura N. Physical attack protection techniques for IC chip level hardware security. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2021, vol. 30, no. 1, pp. 5–14.
98. Gupta R.K. An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G. *Wireless Communications and Mobile Computing*, 2022, vol. 2022, pp. 1–14.

Information about the authors

Semen M. Levin, Cand. Sc., PhD, Professor, Tomsk State University of Control Systems and Radioelectronics, 40, Lenin avenue, Tomsk, 634050, Russian Federation. semen.m.levin@tusur.ru; http://orcid.org/0000-0002-3470-6365

Received: 25.01.2024
Revised: 03.03.2024
Accepted: 29.03.2024

Информация об авторах

Семен Михайлович Левин, кандидат юридических наук, PhD, профессор кафедры автоматизированных систем управления Томского государственного университета систем управления и радиоэлектроники, Россия, 634050, г. Томск, пр. Ленина, 40. semen.m.levin@tusur.ru; http://orcid.org/0000-0002-3470-6365

Поступила: 25.01.2024
Принята: 03.03.2024
Опубликована: 29.03.2024