DOI: https://doi.org/10.15276/hait.07.2024.11
UDC 004.05

Cyber-aware threats and management strategies in cloud environments

Vira V. Liubchenko[1), 2)]
ORCID: https://orcid.org/0000-0002-4611-7832; lvv@op.edu.ua. Scopus Author ID: 56667638800
Denys V. Volkov[1)]
ORCID: https://orcid.org/0009-0006-0933-616X; volkov.denis.v17@gmail.com
[1)] Odessa Polytechnic National University, 1 Shevchenko Ave, Odessa, 65044, Ukraine
[2)] Hochschule für Angewandte Wissenschaften Hamburg, Fakultät Life Sciences, Ulmenliet 20, Hamburg, 21033, Germany

ABSTRACT

The paper provides an overview of cyber threats within cloud computing and proposes effective management strategies. The transition to cloud services has introduced significant security concerns, particularly regarding data protection and privacy. The study aims to catalogue an exhaustive inventory of threats, analyse their prevalence, and thoroughly study applicable security mechanisms. The authors conducted an in-depth literature review, focusing on articles published after 2018, to identify vulnerabilities, attack vectors, and mitigation strategies. The paper categorises various cyber threats, such as malware, phishing, man-in-the-middle attacks, denial-of-service attacks, and SQL injections, and discusses their potential to infiltrate, deceive, disrupt, and steal data. It also highlights the importance of securing internet-connected devices and recommends strategies like robust password policies and regular software updates. The paper concludes by emphasising the need for adaptive security strategies to combat the evolving nature of cyber threats. It advocates for a dynamic approach to security, integrating robust defence mechanisms, continuous monitoring, and rapid response protocols. By prioritising cybersecurity, organisations can navigate the complexities of cloud computing, ensuring their data assets' integrity, confidentiality, and availability in a digital landscape. The findings are a foundation for crafting a security framework tailored to applications operating within cloud environments.

Keywords: Cloud computing; security threats; vulnerabilities; cybersecurity; cloud service provider; software

***For citation*: Liubchenko V. V., Volkov D. V. "Cyber-aware threats and management strategies in cloud environments". *Herald of Advanced Information Technology.* 2024; Vol.7 No.2: 158–170. DOI: https://doi.org/10.15276/hait.07.2024.11**

INTRODUCTION

Today, cloud technologies (otherwise known as cloud computing) have become an indispensable part of our lives. They created a boom in the development of the IT sector, influencing various aspects of modern society. Many business owners and government agencies are switching to cloud technologies, seeing their undeniable advantages.

Cloud computing delivers computing resources over the Internet, including software, data storage, or computing power. This makes it possible to use the services provided by cloud providers remotely, regardless of the client's location. This approach is fundamentally different from traditional on-premises infrastructure.

Two key features of cloud computing are scalability and cost savings. Customers no longer have to purchase and maintain server equipment, which was a costly investment. This allows the client to increase or decrease the resources he needs anytime, reducing the financial burden and optimising the use of cloud resources. The development of cloud technologies is progressing rapidly. Many surveys, reports, and expert assessments confirm this. In recent years, cloud computing has witnessed an unprecedented surge in adoption across various industries.

Despite its many benefits, the widespread adoption of cloud computing raises essential issues related to data security, privacy, and the digital divide. Table 1 provides a short overview of the most known cyberattacks.

As sensitive data is transferred to cloud servers, strong security measures must be in place to protect against hacking and unauthorised access. Therefore, data and service protection issues become particularly relevant.

Our study aims to provide an overview of the state-of-the-art research on security threats within cloud environments. It should support pinpointing outstanding challenges and potential areas for further investigation.

To accomplish this objective, the following tasks should be undertaken:

– conduct an in-depth analysis of pertinent publications to create an exhaustive inventory of threats encountered by cloud environments;

Table 1. **Known cyberattacks**

Year	Goal	Damage
2017	Equifax	A data breach affecting millions of individuals
2018	Strathmore College	The personal records of more than 300 Melbourne high school students were mistakenly published on the school's intranet, causing a privacy breach
2018	Veeam	Inadvertently exposed 200GB of data via an unsecured MongoDB server
2019	Facebook	A breach caused a massive leak of data, including details from 533 million users
2019	Alibaba	A data leak exposing over 1.1 billion user pieces of information
2019	Sina Weibo	Data from 538 million Weibo users has surfaced on the dark web for sale
2021	LinkedIn	A trove of data containing information from over 700 million LinkedIn users was leaked online
2021	Cognyte	As a result of an insecure configuration, a database containing 5 billion user records was exposed
2023	Toyota	Data breach exposing 2.15 million customers' car-location information over ten years due to a database misconfiguration
2023	MGM Resorts	Hackers cyberattack costing $100 million
2023	Dymocks	The breach exposed customer details affecting approximately 1.2 million user records

Source: **compiled by the authors**

– gather data on the prevalence of cyber threats to enhance comprehension of their distribution and characteristics;

– scrutinise security mechanisms and strategies applicable to applications operating in cloud environments.

The rest of the paper is organised as follows: Section II analyses related work, Section III describes the research method used to conduct the mapping study, Section IV presents the study results, Section V discusses the findings, and Section V states the conclusion and future work.

LITERATURE REVIEW

In the ever-evolving landscape of cloud computing, prioritising applications and data security is crucial. This section delves into articles published post-2018 that specifically explored security threats in cloud computing. Concentrating exclusively on cloud infrastructures, the objective is to provide a nuanced exploration of vulnerabilities, attack vectors, and mitigation strategies.

The article [1] traces the evolution of cyber threats from their origins in artificial intelligence to their present-day sophistication, underscoring their increasing complexity and ability to disrupt critical operations and compromise sensitive data. The article categorises and examines various threats, including malware, phishing techniques, man-in-the-middle attacks, denial-of-service (DoS) attacks, and SQL injections. The focus is on elucidating their capacities to infiltrate, deceive, disrupt, and steal data. These discussed threats pose significant risks to both organisations and users.

In [2], the authors delve into the security threats in cloud computing. The article underscores worry regarding data security and privacy when utilising cloud services. It acknowledges the reservations surrounding storing data on servers in other countries, highlighting concerns about potential data breaches, cyber-attacks, unauthorised access, and data loss or corruption risks.

The article [3] explores various security issues and challenges in cloud computing. As well the authors delve into specific security issues prevalent in cloud computing:

– data breaches: the unauthorised exposure of sensitive and confidential data, whether intentional or unintentional, poses a significant security risk;

– account hijacking: attackers compromise cloud user accounts through phishing or malware, utilising stolen accounts for malicious activities;

– insider attacks: malicious actions by insiders that exploit their knowledge of the company's infrastructure to orchestrate attacks;

– DoS attacks: targeted at disrupting cloud services by inundating them with unwanted traffic, DoS attacks compromise accessibility for legitimate users;

– data loss incidents: destroying information systems due to negligence, mishandling, natural disasters, or intentional/unintentional actions by service providers results in critical data loss with potentially severe impacts on businesses.

In [4], authors explored various cyber-attacks, including distributed denial of service (DDoS) attacks, malicious domains, websites, malware, ransomware, spam emails, malicious social media messaging, business email compromise, mobile threats, and risky browsing apps. The article delves into the repercussions of cyber-attacks, outlining potential outcomes such as information loss, financial harm, business disruptions, and threats to the peace and security of affected individuals. Examples underscore the broader societal implications, explicitly focusing on reputational damage for companies. The authors highlighted the significance of securing internet-connected devices to diminish cyber-attack efficacy and fortify defences against potential data breaches and security threats. They recommended strategies such as implementing robust password regulations, creating unique and complex passwords, refraining from sensitive transactions on public Wi-Fi, changing default passwords, keeping software up to date, and regularly backing up personal files.

The article [5] delves into the cyber-attack realm, exploring their origins and presenting various models proposed for detection and defence. Each model employs distinct methods such as tokenisation, stemming, and document term matrices. The article also outlines the limitations and challenges associated with these models. The authors discussed specific types of cyber-attacks: malware, phishing, man-in-the-middle attacks, DoS attacks, SQL injection attacks, zero-day attacks, cross-site scripting, credential reuse attacks, password attacks, and drive-by download attacks. Concise descriptions are provided for each type, offering insights into their nature and characteristics.

The article [6] delved into the significance of cybersecurity across various domains, including backup and data recovery, physical access controls, logical access controls, email and online protection, and vulnerability assessments with security training. The authors elucidated methodologies for detecting malware, covering signature- and behaviour-based approaches. Additionally, they explored phishing detection methods, incorporating rules and obfuscation URL detection. The article strongly emphasised prevention techniques for malware and phishing, advocating for security measures such as regular security patches, cautious online behaviour, strong password practices, firewall implementation, antivirus software usage, and continuous security training.

The authors of [7] introduced the innovative semantically enabled model (CSM) to address cybersecurity issues in cloud computing, incorporating hierarchical ontological structures and intelligent reasoning techniques. The impact analysis of cyber-attacks was explored through the attack-countermeasure tree (ACT), allowing probabilistic analysis. The application of ACT to cloud-based systems was discussed, and integration with the CSM model was proposed for a comprehensive approach.

The article [8] also highlighted the utility of the ACT as a modelling tool for cyber-attacks and countermeasures, facilitating probabilistic analysis. It explored the application of ACT to cloud-based systems and proposed its integration with the CSM model to conduct a comprehensive impact analysis of cyber-attacks.

The research [9] examined various strategies and methods to prevent cyberattacks, explicitly identifying and preventing phishing websites. Specific algorithms such as Cuckoo search, fuzzy logic categorisation, twin support vector machines, convolutional neural networks, and hybrid deep learning networks were discussed in detail. In addition, the article introduces prevalent types of cyberattacks. It underscores the significance of proactive measures and the implementation of access management and robust password practices as effective means to prevent cyberattacks.

The article [10] comprehensively explored various facets of common cyber threats and delved into specific types of DoS attacks. Incorporating examples and statistics, it underscored the risks and potential consequences of these threats for individuals and organisations.

The article [11] explored critical issues within cloud computing, focusing on security and privacy concerns. It underscored information security risks, including the potential loss of data control, compromises to data integrity, and the risk of data seizure. Challenges related to incompatibility when transitioning between cloud vendors and the ongoing evolution of cloud applications were also emphasised. The article addressed the potential ramifications of a cloud provider failure and its impact on data access, advocating for frequent backups as a precautionary measure. In the context of cloud computing, the article delved into network security concerns. Security issues within a virtualised environment are discussed, covering aspects such as the isolation of instances and security measures for both host and guest operating systems. Fundamental security issues like data location awareness, data sanitisation, and potential job depletion due to viruses or worms are outlined.

The study [12] underscores the substantial risks associated with cloud security, identifying them as significant obstacles to the widespread adoption of cloud computing services. Notably, security risks are closely tied to data security issues, including challenges related to data visibility, control, and theft within shared customer data on cloud platforms. The authors delved into specific security threats. The article stressed the imperative for organisations to address threats through robust security measures, policy enforcement, and a clear understanding of the shared nature of cloud resources.

Article [13] addressed security challenges within cloud computing, specifically focusing on concerns related to protection and privacy. It delved into key information security aspects, including data control loss, data integrity, and the risk of data seizure. Network protection is a central theme, encompassing discussions on DDoS attacks, man-in-the-middle attacks, IP spoofing, port filtering, and packet sniffing. General security concerns within this environment are explored, including the separation and isolation of virtual machines and the importance of rigorous monitoring of machine control and access.

Summarising the analysis of published studies, we want to highlight that different authors define the importance of threats differently and offer different solutions. Therefore, a systematic synthesis of the analysed studies should be carried out.

STUDY DESIGN

Summarising published research aims to identify significant patterns and unresolved issues. To this end, two research questions were established:

RQ1. What are the most frequently analyzed threats in cloud environments?

RQ2. What security techniques are commonly used?

For the acquisition of pertinent papers, we applied the following search requests to titles, keywords, and abstracts of articles: (“cybersecurity” OR “threat” OR “attack”) and (“cloud computing” OR “cloud environment”)) with a limited search time interval starting from 2018.

During the study selection stage, we refined the collection derived from the search procedure to exclude articles misaligned with the study objectives. Additionally, any duplicated content was meticulously eliminated. Subsequently, we pruned papers containing less than five pages due to their insubstantial informational content.

For pattern detection, we used clustering and secondary research.

DELIVERED PATTERNS

Distribution of treats mentions

To answer RQ1, we formed the list of treats mentioned in publications. The initial list consisted of 71 treats, most discussed once or twice. Such a result is purely informative, so we grouped similar treats. For this purpose, we applied clustering to three features: threat source, impact object, and implementation mechanism. As a result, we got 17 groups of treats, as shown in Table 2.

Table 2. Groups of threats tackled by the studies

Group of treats	Number of mentions	Sources
DoS	18	[1-2], [6-8], [10-22]
Man-in-the-Middle	14	[1], [6-8], [11-14], [16-18], [20-21], [23]
Malware	11	[1], [4], [6-8], [10-11], [14-15], [17], [21]
SQL Injection	11	[1], [6], [8], [11-12], [14], [16-19], [21]
Spoofing/tampering	11	[7], [10-13], [16-21]
DDoS	11	[1], [5], [7], [10-12], [15], [17-18], [21], [23]
Password/authentication attacks	10	[6-7], [10], [12], [14-18], [21]
Cross-site scripting	9	[6], [11-12], [14], [16-19], [21]
Network attack	9	[6-7], [11-13], [16], [18], [20-21]
VM related attacks	7	[7], [12], [15-19]
Hijacking	7	[11-12], [14-17], [21]
System, application, API, and service threats	7	[7], [11-12], [16-18], [21]
Web application threats	6	[10], [12], [17-19], [21]
Cloud-related attacks	5	[12], [15-18]
Eavesdropping attack	4	[11-12], [15], [18]
Wireless network security	1	[21]
Other	6	[7], [11-12], [17-18], [21]

Source: **compiled by the authors**

Denial of Service (DoS)

DoS is the most frequently discussed threat group. A DoS attack is a malicious attempt to disrupt the normal operations of a targeted system or network by flooding it with excessive traffic or requests, rendering it unable to fulfil legitimate requests. These attacks can vary in complexity and scale. Still, their fundamental goal is to overwhelm the target's resources, such as bandwidth, processing power, or memory, disrupting services.

DoS attacks typically involve flooding systems, servers, or networks with overwhelming traffic or requests, causing them to become unavailable to legitimate users. This flood of traffic overloads the target's resources, making it unable to process and respond to genuine requests.

Some common subtypes of DoS attacks include:

– Ping of death. In this type of attack, the attacker sends malformed or oversized packets, exceeding the maximum allowable size limit, to crash the target system. By fragmenting the IP packets, attackers aim to cause buffer overflows and other system crashes when the target system reassembles the packets.

– Teardrop attack. This attack involves sending fragmented packets to the target machine. Since the receiving machine cannot reassemble these packets correctly, they overlap, leading to a crash of the target network device. Although rare today, older operating systems may still be vulnerable to this attack.

– LAND attack. This attack involves sending spoofed SYN packets with the same source and destination IP addresses, causing the target system to crash.

– SMURF attack. This attack leverages ICMP echo requests to flood a target network with responses, causing congestion and rendering it inaccessible to legitimate users.

– SYN flood. In this attack, the attacker floods the target system with spoofed SYN packets, exhausting its resources and preventing it from processing legitimate connection requests.

DoS attacks can have severe consequences, particularly in cloud computing environments where services are shared among numerous users. These attacks can disrupt service availability, degrade performance, and incur financial losses for affected organisations. Additionally, the proliferation of botnets has made it easier for attackers to execute large-scale DoS attacks, amplifying their impact and making them more challenging to mitigate.

Distributed Denial of Service (DDoS)

Curiously, the DDoS group is referenced nearly half as frequently. A DDoS attack is a cyber assault orchestrated by multiple compromised host machines. The objective is to disrupt the normal functioning of a targeted network, server, or service by overwhelming it with a flood of internet traffic. These attacks aim to cause service denial, effectively rendering the target inaccessible to legitimate users. Common DDoS attacks include TCP SYN flood, tear attack, smurf attack, UDP flood attack, ICMP attack, and botnets. Subtypes of DDoS attacks include HTTP flooding, which exploits legitimate HTTP requests, and Zero Day attacks, which exploit unknown security vulnerabilities.

DDoS attacks can severely impact the normal flow of traffic to a targeted network, server, or service. This disruption is akin to a traffic jam that prevents legitimate traffic from reaching its intended destination. In cloud environments, DDoS attacks pose significant threats, affecting availability and security and consuming processing power, which may have financial implications for cloud customers.

Man-in-the-Middle (MitM)

A MitM attack is a cyber-attack where an unauthorised third party intercepts and possibly alters the communication between two parties without their knowledge. The attacker positions themselves between the two communicating parties, secretly monitoring and potentially manipulating the data being exchanged. The main goal of a MitM attack is to obtain sensitive information such as personal data, passwords, and financial information or to impersonate one of the parties involved.

Several techniques can be employed in a MitM attack, including session hijacking, IP spoofing, replay attacks, and intercepting unencrypted data packets. Typical scenarios where MitM attacks occur include insecure public Wi-Fi networks or compromised network infrastructure.

MitM attacks pose severe threats to data security and privacy, as the attacker can access and manipulate sensitive information exchanged between the victims.

Malware

External threats receive considerable attention. A malware attack is the deliberate deployment of malicious software onto a computer, server, client, or computer network to cause harm, disrupt operations, compromise security, or steal sensitive information. Malware encompasses many programs, including viruses, worms, trojans, ransomware,

spyware, adware, and rootkits. These programs exploit vulnerabilities in systems and networks, often infiltrating them without the user's knowledge or consent.

Common types of malware include macro viruses, file infectors, system or boot-record infectors, polymorphic viruses, stealth viruses, logic bombs, droppers, adware, spyware, and trojan horses. These malicious programs vary in their propagation methods and the types of harm they cause, ranging from unauthorised data collection to system damage and network disruption.

Trojan horses masquerade as legitimate software but contain malicious payloads, often leading to unauthorised data collection or system damage. Computer viruses replicate and spread by attaching themselves to other files or programs, altering their behaviour. Computer worms are self-replicating malware that spread across networks, exploiting vulnerabilities to infect other systems. Rootkits provide unauthorised access and control over a victim's device, often hidden to evade detection.

SQL injection

An SQL injection attack occurs when an attacker inserts malicious code into a server using Structured Query Language (SQL), compelling the server to deliver sensitive information. This attack typically involves injecting malicious code into an unprotected website comment or search box. SQL injection poses a significant threat to web-based systems, allowing attackers to manipulate databases, steal sensitive data like credit card details or usernames and passwords, and even gain unauthorised access to the system. Developers must know SQL injection attacks and implement proper input validation and security measures to mitigate this vulnerability. Secure coding practices, such as using prepared statements with parameterised queries, can prevent SQL injections. When SQL commands use parameters instead of embedding values directly, it can prevent the backend from executing malicious code.

Cross-Site Scripting (XSS)

An XSS attack occurs when malicious code is injected into a trusted website, typically a client-side script. The attacker embeds malicious scripts into the website's content or database. When a user visits the compromised page, their browser unknowingly executes the injected script, as it appears to originate from a trusted source. This allows the attacker to access sensitive information, such as session tokens and cookies. The consequences of XSS attacks can range from capturing keystrokes and screenshots to gaining unauthorised access to the victim's machine. These attacks exploit vulnerabilities in web applications, particularly those using dynamic web pages and JavaScript. Preventive measures against XSS attacks include enforcing a no-script policy on untrusted HTML, proper Secure Socket Layer configuration, anti-malware software, browser collaboration, and content-based data leakage prevention technology.

Spoofing

Spoofing involves manipulating data or communication to deceive a recipient into believing it originates from a trusted source when it does not. There are various forms of spoofing, such as metadata spoofing, IP spoofing, and ARP spoofing, each targeting different aspects of communication systems.

In metadata spoofing, the attacker tampers with service descriptions, affecting service confidentiality and potentially altering service functionalities. This can lead to unauthorised access or modification of sensitive information.

IP spoofing involves an attacker impersonating a trusted entity by altering the source IP address of network packets. This can trick a target host into accepting the packets as legitimate, enabling unauthorised access to systems, or facilitating attacks like flooding to overwhelm network resources.

While operating at the data link layer, ARP spoofing involves falsifying ARP messages to associate a spoofed MAC address with a legitimate IP address. This allows the attacker to intercept or manipulate network traffic, bypassing network security measures or gaining unauthorised access to systems.

Spoofing attacks exploit network protocol or service vulnerabilities, often aiming to gain access to sensitive information, spread malware, bypass security controls, or disrupt services through denial-of-service attacks. Measures such as ingress filtering can help mitigate the risks associated with spoofing attacks, but preventing spoofed packets from infiltrating networks remains challenging.

Password Attack

A password attack is a method used by attackers to gain unauthorised access to someone's private accounts by exploiting weaknesses in password security. These attacks exploit vulnerabilities such as credential reuse, password guessing, password resets, credential exposure, and password discovery. Credential reuse attacks occur

when individuals reuse the same password across multiple accounts, making it easier for attackers to access numerous accounts if one is compromised. Password guessing involves systematically trying different password combinations, including commonly used ones found in dictionaries or based on personal information about the user. Password reset attacks involve trying out every possible combination of characters to guess the password, often aided by tools that can expose strongly encrypted data. Credential exposure refers to attackers obtaining usernames and passwords from hacked websites or other sources and using them to gain unauthorised access. Password discovery attacks involve attempting to discover passwords through various means, such as phishing, fraud, or exploiting software flaws. To mitigate password attacks, it's essential to adopt strong password security practices, including using unique passwords for each account, regularly changing passwords, and employing multi-factor authentication where possible. Additionally, organisations should implement robust authentication and access control methods, encrypt transmitted data, and continuously monitor and update security measures to protect against evolving threats.

We won't delve into the other identified groups extensively. We only note that we were surprised by the emergence of wireless network security threats within cloud environments. These encompass SSID issues, WEP vulnerabilities, MAC attacks, STP attacks, and jamming. Notably, all these threats originate “externally” in the cloud environment.

Comparison with empirical rankings

Checking rankings of security threats in cloud computing through dedicated resources or platforms offers several advantages compared to relying solely on research articles. These platforms provide real-time updates on cloud computing security threats, vulnerabilities, and incidents, ensuring users can access the most current information. They aggregate data from various sources, including industry reports, incident databases, security advisories, and research articles, offering a broader perspective on the landscape of security threats. They typically provide a vendor-neutral perspective on security threats, enhancing the credibility and trustworthiness of the information provided. We analysed three threat rankings (Table 3).

The frequency distribution obtained from articles and research papers encompasses a broader spectrum of cyber threats than those provided by specialised internet sources. While the specialised sources primarily focus on specific vulnerabilities and risks within cloud computing environments, the research-based frequency distribution includes a more comprehensive range of threats affecting various aspects of cybersecurity.

However, there are some commonalities and potential dependencies that can be observed:

– SQL injection: the SANS Institute's List mentions this threat as “Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')”;

– password/authentication attacks: this category aligns with the identity, credentials, and access management concerns the Cloud Security Alliance highlighted;

– XSS: XSS attacks are listed in SANS Institute's and OWASP's statistics, indicating their significance as a common threat to web applications and cloud environments;

– system, application, API, and service threats: this category broadly aligns with several threats highlighted by the Cloud Security Alliance, SANS Institute, and OWASP, such as insecure interfaces, software vulnerabilities, and misconfigurations;

– web application threats: the statistics from OWASP's list address web application threats, which include vulnerabilities like injection, broken access control, and insecure design;

– cloud-related attacks: The rankings from the Cloud Security Alliance's list implicitly address cloud-related attacks, which include threats specific to cloud environments, such as misconfigurations and inadequate security architecture.

Security techniques

To answer RQ2, we formed the list of security techniques mentioned in publications. All security techniques against threats inherent in applications deployed in cloud environments were divided into three groups depending on who should implement them without delving into specific implementations (Table 4).

Independent of the cloud provider/application. These defence strategies are within the user's or organisation’s control and can be implemented regardless of the specific cloud service provider or application. They focus on user behaviour, organisational policies, and proactive security measures.

Table 3. **Analyzed threat rankings**

"Top threats to cloud computing pandemic eleven" of Cloud Security Alliance [24]	List of SANS Top 25 critical vulnerabilities in software [25]	OWASP's 2021 security risk statistics [26]
1. Insufficient identity, credentials, access, and key management 2. Insecure interfaces and APIs 3. Misconfiguration and inadequate change control 4. Lack of cloud security architecture and strategy 5. Insecure software development 6. Unsecured third-party resources 7. System vulnerabilities 8. Accidental cloud data disclosure 9. Misconfiguration and exploitation of serverless and container workloads 10. Organized crime/hackers/APT 11. Cloud storage data exfiltration	1. Out-of-bounds write 2. Improper neutralization of input during web page generation ("Cross-site Scripting") 3. Improper neutralization of special elements used in an SQL command ("SQL Injection") 4. Use after free 5. Improper neutralization of special elements used in an OS command ("OS Command Injection") 6. Improper input validation 7. Out-of-bounds read 8. Improper limitation of a pathname to a restricted directory ("Path Traversal") 9. Cross-site request forgery (CSRF) 10. Unrestricted upload of file with dangerous type 11. Missing authorization 12. NULL pointer dereference 13. Improper authentication 14. Integer overflow or wraparound 15. Deserialization of untrusted data 16. Improper neutralization of special elements used in a command ("Command Injection") 17. Improper restriction of operations within the bounds of a memory buffer 18. Use of hard-coded credentials 19. Server-side request forgery (SSRF) 20. Missing authentication for critical function 21. Concurrent execution using shared resources with improper synchronisation ("Race Condition") 22. Improper privilege management 23. Improper control of generation of code ("Code Injection") 24. Incorrect authorisation 25. Incorrect default permissions	1. Broken access control 2. Cryptographic failures 3. Injection 4. Insecure design 5. Security misconfiguration 6. Vulnerable and outdated components 7. Identification and authentication failures 8. Software and data integrity failures 9. Security logging and monitoring failures 10. Server-side request forgery (SSRF)

Source: **compiled by the authors**

Table 4. **Security techniques**

Independent of the cloud provider/application	Dependent on the cloud provider	Dependent on the application
1. Strong password 2. Do not use suspicious links and emails 3. Security development lifecycle 4. Iterative approach to critical component identification 5. Sandboxing 6. Formal change control process 7. Different types of agreements 8. Third-party auditing 9. Staff training	1. Traffic analysis/monitoring 2. Anti-malware protection 3. Software updates 4. Backup creation 5. Intrusion detection systems 6. Intrusion prevention systems 7. Sensitive data tokenization 8. Sensitive data encryption 9. Data hashing 10. Authorization and authentication mechanisms 11. Access management 12. Vulnerability scanning tools 13. Key management 14. Anti-crawler mechanisms 15. Network configuration 16. Security protocols (Protocol encryption) 17. Trust management 18. Searchable encryption 19. Secure data destruction 20. SQL injection mitigation strategies 21. XSS injection mitigation strategies 22. Port-scanning mitigation strategies 23. Penetration testing 24. Secure web gateway 25. Firewall 26. DDoS mitigation strategies 27. Endpoint protection 28. Command and control (2C) mitigation strategies 29. VM-related issues mitigation strategies 30. Cloud virtualization schemes	1. Traffic analysis/monitoring 2. Anti-malware protection 3. Software updates 4. Backup creation 5. Intrusion detection systems 6. Intrusion prevention systems 7. Sensitive data tokenization 8. Sensitive data encryption 9. Data hashing 10. Authorization and authentication mechanisms 11. Access management 12. Vulnerability scanning tools 13. Key management 14. Anti-crawler mechanisms 15. Network configuration 16. Security protocols (Protocol encryption) 17. Trust management 18. Searchable encryption 19. Secure data destruction 20. SQL injection mitigation strategies 21. XSS injection mitigation strategies 22. Port-scanning mitigation strategies 23. Penetration testing 24. Secure web gateway 25. Ingress filtering

Source: **compiled by the authors**

Dependent on the cloud provider. These defence strategies rely on the cloud service provider's services and features. While users may have some control over their configuration and management, the cloud provider offers the core functionality.

Dependent on the application. These defence strategies are specific to the application or software running on the cloud infrastructure. The developers of this application must implement these techniques.

The “Dependent on the cloud provider” and "Dependent on the application” groups share many similarities because of their shared objective: ensuring the security of the overall cloud environment and its applications. While these two groups may appear distinct, they often intersect due to their interconnected nature within the cloud infrastructure. Cloud service providers often offer security services and features that can be leveraged by applications deployed on their platforms. For example, cloud providers may provide built-in firewall solutions, DDoS protection, encryption services, and identity and access management tools

that applications can utilise to enhance their security posture.

However, developers can implement their security solutions instead of relying solely on the tools provided by cloud service providers.

There are several reasons why a developer may opt for custom security solutions:

– specific security requirements: an application's security requirements may vary based on industry regulations, data sensitivity, and compliance standards;

– advanced security needs: some applications may require advanced security measures or specialised security controls unavailable through standard cloud provider offerings;

– integration with existing systems: custom security solutions can be tailored to integrate seamlessly with existing systems, applications, and workflows;

– complete control and customisation: building custom security solutions gives developers complete control over the design, implementation, and management of security measures;

– cost considerations: while cloud provider security services offer convenience and scalability, they may come with associated costs. In some cases, custom security solutions may be more cost-effective, particularly for applications with unique security requirements or long-term operational considerations.

On the other hand, the cloud provider is responsible for securing the underlying infrastructure and platform, and application developers are responsible for securing the applications they deploy on the cloud. For example, a firewall. Its implementation on the side of the cloud providers and applications is radically different, although the same term also refers to them.

DISCUSSION

The discourse surrounding security threats in cloud computing underscores the critical need for proactive measures to mitigate risks and safeguard sensitive data. The comprehensive analysis of prevalent threats, ranging from malware and phishing attacks to DoS attacks and SQL injections, illuminates the multifaceted challenges organisations in cloud environments face.

The riskier a particular threat is considered by researchers, the more often it is mentioned in publications. The level of risk determines the expected level of losses and the probability of the threat materialising.

One of the paramount considerations highlighted in this study is the evolving nature of cyber threats and the need for adaptive security strategies. Traditional security approaches may prove inadequate as cybercriminals refine their tactics and exploit vulnerabilities. Therefore, stakeholders must adopt a dynamic and multifaceted approach to security, integrating robust defence mechanisms, continuous monitoring, and rapid response protocols.

Moreover, the comparisons with specialised internet sources highlight commonalities in identified threats, providing valuable insights into the evolving cybersecurity landscape. This synthesis of diverse perspectives offers a holistic understanding of the prevailing security challenges in cloud computing and informs strategic decision-making processes.

Furthermore, exploring security techniques categorised by implementation dependencies elucidates the diverse measures available to bolster cloud security. While cloud service providers offer essential security features, organisations must complement these with user-controlled and application-specific solutions tailored to their unique requirements. By embracing a layered defence strategy, organisations can enhance their resilience to emerging threats and mitigate the potential impact of security breaches.

CONCLUSION

In conclusion, this research underscores the imperative for proactive security measures and collaborative efforts among stakeholders to fortify cloud environments against evolving threats. By prioritising cybersecurity and adopting a proactive stance, organisations can confidently navigate the complexities of cloud computing, ensuring the integrity, confidentiality, and availability of their data assets in an increasingly interconnected digital landscape.

During an in-depth analysis of published research, 71 threats related to working in cloud environments were identified and clustered into 17 groups. Rankings were constructed for these groups to reflect the level of risk associated with each threat group. Additionally, data for each group of threats was collected to enhance understanding of their distribution and characteristics.

Studying security mechanisms and strategies

implemented in applications within cloud environments enabled identifying three groups based on existing dependencies. Despite conducting a thorough analysis of publications, no dependencies between threats and security mechanisms were discerned. Nonetheless, it can be contended that priority should be given to methods within the application-dependent group when crafting software.

The findings from this analysis serve as the foundation for crafting a security framework tailored to applications operating within cloud environments.

REFERENCES

1. Nayak, P., Sufiyan, M., N S, M., Bhaskar, M. G. & Raju, M. “Review paper on cyber security and types of cyber attacks”. *International Journal of Advanced Research in Science, Communication and Technology*. 2022; 2 (1): 732–735. DOI: https://doi.org/10.48175/ijarsct-7043.

2. Razi, M. & Batan, A. “Opportunities and challenges of cloud computing in developing countries”. *Artificial Intelligence in Society.* 2023; 3 (1): 1–8.

3. Walling, S. “A Comprehensive review on cloud computing and cloud security issues”. *International Journal of Advanced Research in Science, Communication and Technology*. 2020; 6 (4): 483–490. DOI: https://doi.org/10.32628/CSEIT206489.

4. Mohamad Fadli, Z., Yong, S. S., Kee, L. K. & Ching, G. H. “Cyber attack awareness and prevention in network security”. *International Journal of Informatics and Communication Technology.* 2022; 11 (2): 105–115. DOI: https://doi.org/10.11591/ijict.v11i2.pp105-115.

5. Deepak, M. D., S Kumar, B. & Lal, D. “Major hurdles of cyber security in 21st Century”. *International Journal of Engineering and Advanced Technology.* 2020; 9 (3): 1470–1476. DOI: https://doi.org/10.35940/ijeat.C5135.029320.

6. Vakil, J. & Swaminarayan, Dr P. “Cyber Attacks: Detection and Prevention”. *International Journal of Scientific Research in Science, Engineering and Technology.* 2022; 9 (5): 82–93. DOI: https://doi.org/10.32628/ijsrset229511.

7. Ganesh, E. N. “Study on anomaly cyber attacks on cloud systems”. *Environment*. 2022; 5: 7–12. DOI: https://doi.org/10.6084/m9.figshare.21291582

8. Subrmaniam, G. “Analysis of cyber attacks in cloud technology”. *International Journal of Microelectronics and Digital Integrated Circuits.* 2022; 3 (2). DOI: https://doi.org/10.6084/m9.figshare.21505743.

9. Baballe, M. A., Hussalni, A., Bello, I. & Musa, U. “Current trends in information technology online attacks types of data breach and cyber-attack prevention methods”. *Current Trends in Information Technology.* 2022; 12 (2): 21–26. DOI: https://doi.org/10.37591/CTIT.

10. Haidros, H. & Naik S, M. “An overview on cyber attacks: Impacts and mitigations”. *Data Mining & Predictive Analytics.* 2021. p. 69–84.

11. Onyarin, O. J. & Ese, M. S. “A review of security issues in cloud computing”. *Web of Deceit*. 2022. p. 279–290. DOI: https://doi.org/10.22624/AIMS/BK2022-P47.

12. Hassan, W., Chou, T., Tamer, O., Pickard, J., Appiah-Kubi, P. & Pagliari, L. “Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science”. *International Journal of Informatics and Communication Technology.* 2020; 9 (2): 117–139. DOI: https://doi.org/10.11591/ijict.v9i2.pp117-139.

13. Shyam, G. K. & Ansari, M. A. S. “Security concerns in cloud computing”. *International Journal of Trend in Scientific Research and Development.* 2018; 2 (5): 2296–2301. DOI: https://doi.org/10.31142/ijtsrd18306.

14. Viganò, E., Loi, M. & Yaghmael, E. “Cybersecurity of critical infrastructure". *The Ethics of Cybersecurity.* 2020. p. 157-77. https://www.scopus.com/authid/detail.uri?authorId=57194203025. DOI: https://doi.org/10.1007/978-3-030-29053-5_8.

15. Abdulsalam Y. S. & Hedabou M. “Security and Privacy in Cloud Computing: Technical Review”. *Future Internet*. 2021; 14 (1), https://www.scopus.com/authid/detail.uri?authorId=57221383735. DOI: https://doi.org/10.3390/fi14010011.

16. Hassan, W., Chou, T., Li, X., Appiah-Kubi, P. & Tamer, O. “Latest trends, challenges and solutions in security in the era of cloud computing and software-defined networks”. *International Journal of*

Informatics and Communication Technology. 2019; 8 (3): 162–183. DOI: https://doi.org/10.11591/ijict.v8i3.pp162-183.

17. Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A. & Praveen, S. "A comprehensive overview of privacy and data security for cloud storage". *International Journal of Scientific Research in Science, Engineering and Technology*. 2021; 8 (5): 113–152. DOI: https://doi.org/10.32628/IJSRSET21852.

18. Alhenaki, L., Alwatban, A., Alahmri, B. & Alarifi, N. "Security in cloud computing: A Survey". *International Journal of Computer Science and Information Security.* 2019; 17 (4): 67–90.

19. Tabrizchi, H. & Rafsanjani, M. K. "A survey on security challenges in cloud computing: issues, threats, and solutions". *The Journal of Supercomputing.* 2020; 76 (12): 9493–9532, https://www.scopus.com/authid/detail.uri?authorId=57208279753. DOI: https://doi.org/10.1007/s11227-020-03213-1.

20. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S. & Sarkar, P. "Cloud computing security challenges & solutions-a survey". *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).* 2018, https://www.scopus.com/authid/detail.uri?authorId=57209613438
DOI: https://doi.org/10.1109/ccwc.2018.8301700.

21. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A. & Akin, E. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions". *Electronics.* 2023; 12 (6): 1–42, https://www.scopus.com/authid/detail.uri?authorId=57201115541
DOI: https://doi.org/10.3390/electronics12061333.

22. Shpinareva, I M., Yakushina, A. A., Voloshchuk, L. A. & Rudnichenko, N. D. "Detection and classification of network attacks using the deep neural network cascade". *Herald of Advanced Information Technology.* 2021; 4 (3): 244–254. DOI: https://doi.org/10.15276/hait.03.2021.4.

23. Surkov, S. S. "Comparison of authorization protocols for large requests in the operation queue environment". *Herald of Advanced Information Technology.* 2020; 3 (3): 163–173. DOI: https://doi.org/10.15276/hait.03.2020.5.

24. "Top threats to cloud computing pandemic eleven". CSA. 2022. – Available from: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven. – [Accessed: 20.03.2024].

25. "Top 25 Software Errors". SANS Institute. 2021. – Available from: https://www.sans.org/top25-software-error/. – [Accessed: 20.03.2023].

26. "OWASP Top Ten". OWASP Foundation. 2021. – Available from: https://owasp.org/www-project-top-ten. – [Accessed: 20.03.2023].

Conflicts of Interest: The authors declare no conflict of interest

Received 11.03.02.2024
Received after revision 10.05.2024
Accepted 16.05.2024

DOI: https://doi.org/10.15276/hait.07.2024.11
УДК 004.05

Кіберзагрози та стратегії їх подолання в хмарних середовищах

Любченко Віра Вікторівна[1),2)]
ORCID: https://orcid.org/0000-0002-4611-7832; lvv@op.edu.ua. Scopus Author ID: 56667638800
Волков Денис Володимирович[1)]
ORCID: https://orcid.org/0009-0006-0933-616X; volkov.denis.v17@gmail.com.
[1)] Національний університет «Одеська політехніка», пр. Шевченка 1. Одеса, 65044, Україна
[2)] Університет прикладних наук, Факультет наук про життя, вул. Ульменліт 20. Гамбург, 21033, Німеччина

АНОТАЦІЯ

У статті подано огляд кіберзагроз у хмарних середовищах та запропоновано ефективні стратегії управління ними. Перехід до хмарних сервісів спричинив значні проблеми з безпекою, особливо щодо захисту даних та забезпечення їх

конфіденційності. Метою дослідження є каталогізація вичерпного переліку загроз, аналіз їх поширеності та ретельне вивчення застосовних механізмів безпеки. Автори виконали огляд літератури, зосередившись на статтях, опублікованих після 2018 року, для виявлення вразливостей, векторів атак та стратегій пом'якшення наслідків. У статті класифіковано різні кіберзагрози, такі як шкідливе програмне забезпечення, фішинг, атаки типу "людина посередині", атаки типу "відмова в обслуговуванні" та SQL-ін'єкції, та обговорено їхній потенціал для проникнення, обману, порушення та викрадення даних. Також підкреслюється важливість захисту пристроїв, підключених до Інтернету, і рекомендуються такі стратегії, як надійна політика паролів і регулярне оновлення програмного забезпечення. Насамкінець наголошується на необхідності адаптивних стратегій безпеки для боротьби з кіберзагрозами, що постійно змінюються. Рекомендовано динамічний підхід до безпеки, що включає надійні механізми захисту, постійний моніторинг і протоколи швидкого реагування. Надаючи пріоритет кібербезпеці, організації можуть орієнтуватися в складнощах хмарних обчислень, забезпечуючи цілісність, конфіденційність і доступність своїх інформаційних активів у цифровому середовищі. Отримані результати є основою для створення системи безпеки, адаптованої до застосунків, що працюють у хмарних середовищах.

Ключові слова: хмарні обчислення; загрози безпеці; вразливості; кібербезпека; провайдер хмарних послуг; програмне забезпечення

ABOUT THE AUTHORS

Vira V. Liubchenko - Doctor of Engineering Sciences, Professor, Department of Software Engineering, Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine; Lecturer, Fakultät Life Sciences, Hochschule für Angewandte Wissenschaften Hamburg, Ulmenliet 20, Hamburg, 21033, Germany
ORCID: https://orcid.org/0000-0002-4611-7832; lvv@op.edu.ua. Scopus Author ID: 56667638800
Scientific field: Data science; software engineering; project management

Любченко Віра Вікторівна - д-р техніч. наук, професор кафедри Інженерії програмного забезпечення Національного університету «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Denys V. Volkov - Postgraduate student, Department of Software Engineering, Odessa Polytechnic National University, 1, Shevchenko Ave. Odessa, 65044, Ukraine
ORCID: https://orcid.org/0009-0006-0933-616X; volkov.denis.v17@gmail.com
Scientific field: Software engineering; cyber security

Волков Денис Володимирович - аспірант кафедри Інженерії програмного забезпечення Національного університету «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна