Journal homepage: https://devma.com.ua/en

DEVELOPMENT MANAGEMENT

UDC 004.056:004.7
DOI: 10.57111/devt/1.2024.37

Vol. 23, No. 1. 2024

Security in cloud computing: Methods for ensuring privacy and integration in modern applications

Oleksii Zarichuk*

Computer and Information Systems Manager
LLC Fides
02000, 11A E. Sverstyuk Str., Kyiv, Ukraine
https://orcid.org/0009-0009-0771-8465

Abstract. Cloud computing has become a necessary component for data storage and processing and is becoming more widespread. However, there are threats to the security and privacy of user data, which is why it is important to find out the most effective methods for ensuring data security in the cloud. The purpose of the study was to develop methods aimed at ensuring privacy and security in cloud environments and in modern applications. The method of analysis was used to review other publications on the topic, and the method of experiment was used for practical implementation. The main results of the study include the development of a security monitoring programme. It analyses event logs and determines the number of failed login attempts, which indicates the detection or absence of suspicious activity. Access to resources is checked, and the necessary information is displayed on the console. A comparison table of cloud platforms has been created, considering their advantages and disadvantages in the context of data security and privacy. It specifies the criteria for delivering services to the selected services. A block diagram of ways to provide security in cloud computing is developed, illustrating the relationship between various aspects of providing security in cloud systems. It contains parameters and strategies for encrypting data, protecting sensitive data, and countering attacks. Various aspects of security and methods of ensuring privacy in cloud computing are considered, namely authorisation, intrusion detection, regulatory requirements, integration with modern applications, monitoring and logging, user identification and authentication. The practical significance of the study lies in the creation of innovative ways to help improve security and privacy in cloud computing. They will allow cloud developers and administrators to effectively protect user data and ensure their privacy in modern applications

Keywords: online payments; data protection; privacy assurance; security of up-to-date applications; virtual environment

Article's History: Received: 22.08.2023; Revised: 06.02.2024; Accepted: 22.03.2024

INTRODUCTION

A large amount of personal and corporate data is stored in cloud environments, so it is important to ensure that it is protected from potential threats. Criminals and hackers are constantly looking for opportunities for unauthorised access to data. Loss or leakage of sensitive information can have serious consequences for users and organisations, enterprises, and administrative institutions specifically. Information security becomes key, in particular, considering mandatory regulatory requirements and standards. Security threats in cloud computing include the possibility of attacks on the infrastructure of cloud systems, violations of regulatory requirements for data protection. These threats can lead to serious consequences for businesses, including financial losses, loss of confidential information, and privacy violations.

Other studies on this topic are of interest. For example, O. Vakhula & I. Opirsky (2023) consider the "Security as a code" approach in cloud environments, which involves integrating security controls directly into software development processes. The researchers emphasise that embedding security measures in programme code, templates, and automated processes guarantees consistent and mandatory implementation of security controls at all stages of development. This approach is an important strategy for ensuring security in cloud environments and plays a role in protecting digital assets. V. Bohomia & V. Kochegarov (2023)

Suggested Citation:
Zarichuk, O. (2024). Security in cloud computing: Methods for ensuring privacy and integration in modern applications. *Development Management,* 23(1), 37-45. doi: 10.57111/devt/1.2024.37.

*Corresponding author

focus on cybersecurity, which is becoming increasingly relevant in Ukraine due to its growing reliance on technology and war-related threats. The increased use of cloud services leads to an increase in cybersecurity threats, especially in terms of privacy and data protection. The study aims to analyse the possibilities of using cryptographic methods to ensure security in cloud services. V. Mazur (2023) implements effective security methods for Amazon Web Services (AWS) cloud services to protect against various types of cyber-attacks. The paper includes an analysis of cyber threats, characteristics and consequences of cyber-attacks, and a study of the advantages and limitations of using AWS cloud services. The proposed security methods include the installation of firewalls, intrusion detection systems, data encryption, backups and recovery, authentication and authorisation of users, improving the security and reliability of the AWS cloud infrastructure against cyber-attacks. Similar is the study by A. Nafiiev & D. Lande (2023), where the researchers consider two methods for controlling malware intrusion recognition. Based on calculations, researchers have created a model for detecting virus programmes based on artificial intelligence (AI). It was noted that to get an optimal result, it is better to use a narrow sample among the entire set of features instead of a large amount of data.

L. Sultanova & M. Prokofieva (2022) substantiate the need to improve digital security in the field of higher education against the background of the threat of spreading fake information. The paper analyses the problem of spreading fake content in Ukraine and highlights ways to combat it. The researchers also consider the concept of digital competence for Ukrainian citizens and suggest improving digital education for teachers and students on digital security issues. In turn, M. Horodyskyi *et al*. (2021) examine the impact of cloud technologies on the organisation of accounting and its regulatory framework. It is noted that the introduction of information and computer technologies in accounting will lead to the reform of its technical and administrative components. The impact of cloud technologies on the organisation of accounting is considered in the aspect of using their advantages and disadvantages. T. Amro (2022) examines the relationship between information security and public administration systems during martial law and examines methods for ensuring effective information security in these conditions. The researcher uses empirical and theoretical methods, including analysis of legal acts regulating these systems. The paper is original because it addresses an under-studied issue and proposes new approaches to ensuring information security under martial law.

All of the above papers focus on security in the cloud, but this study focuses on the importance of integrating security directly into software development processes in cloud environments, which was previously poorly understood. The scope of the study should include the integration of security into modern applications that use cloud computing: this is important because many applications exchange data with cloud systems, and their developers must ensure that this data exchange is secure. The purpose of this study was to develop methods aimed at improving the level of privacy and security in the cloud environment and modern applications.

MATERIALS AND METHODS

The methods of analysis and experiment were used to achieve the research objective. The analysis was used to review other publications and scientific sources on this topic. This analysis helped to clarify existing security approaches and developments in cloud computing, and identify shortcomings and opportunities for further research. This method covered various aspects, including cryptographic methods, security methods for cloud services, firewall settings, unauthorised access detection systems, determining user access rights, backup and data recovery, the problem of fake content spread, ways to improve digital education, the impact of cloud technologies on accounting, analysis of legal acts, and ensuring information security under martial law. The issues of access control and identity management, the role of cloud service providers, various methods of ensuring data privacy, internal threats, data leaks, illegal access to sensitive information, legal and standard requirements for protecting user data in cloud environments were also considered. Some of these aspects include PRISMA approaches, Fog computing, Internet of Things (IoT) devices, scalability, flexibility, reliability, efficiency and outsourcing, and secure configuration, multi-factor authentication, regular audits, security testing, incident response plans, data security and integrity, service level agreements and staff training.

The experimental method was applied for the practical implementation of this topic. The code was written in Java, which is a console application for security monitoring. This programme analyses event logs and checks access to resources to detect suspicious actions. If the number of failed login attempts exceeds a certain value, the application displays suspicious activity, otherwise – suspicious activity is not detected. The code contains a method for checking access to resources, a function for getting the number of failed login attempts from event logs, a function for checking file access, and a function for checking user authorisation. The study also used a structural diagram of these methods of ensuring security in cloud computing, which was created using the Drawio tool. It used data encryption, protection against attacks on third-party code, methods for protecting confidential data, methods for data backup and recovery, threat monitoring and response systems, cryptographic methods, network protocol protection, integration with identification systems, and other methods for providing security in cloud computing. In addition, a comparison table of the leading cloud environments – AWS, Google Cloud Platform (GCP), Microsoft Azure, Salesforce – was created using the comparison and the graphical method. This was done to assess their main characteristics. This table summarised the listed services based on such criteria as the platform name, main services, advantages and disadvantages. The use of the comparison contributed to obtaining an objective comparative overview of well-known cloud platforms, which helped to determine which of them best meets the security requirements.

RESULTS

Cloud computing provides convenient access to resources and data over the Internet and allows efficient use of computing resources without significant investment in own servers and infrastructure. However, along with the growing popularity of cloud computing, the risk of data security and privacy is also growing. Criminals are constantly looking for opportunities to access this data, which leads to serious consequences for users. Key security aspects in cloud computing include data encryption, physical security and infrastructure, authentication and authorisation, incident detection and response, and regulatory requirements and standards.

Encryption is one of the key methods of ensuring privacy. It allows protecting personal data from unauthorised access, even if criminals gain physical access to the data warehouse. Ensuring the security of the physical infrastructure where servers and computing resources are stored is important to prevent physical access to data. It is necessary to protect access to resources and data by authenticating users and controlling access using authorisation tools. Attention should be paid to intrusion detection systems, methods for responding to possible threats, and data protection requirements that are regulated by legislation and standards. Integration with modern applications is another important component for ensuring security in cloud computing. Since many modern applications share data with cloud systems, developers must ensure that this data exchange is secure.

When implementing cloud solutions and defining methods for ensuring security and privacy in cloud systems, certain advantages and disadvantages should be considered. Benefits may include ease of access, cost, scalability, automation and updates, backup and recovery. Cloud computing allows users to access data and resources from anywhere with an Internet connection, which promotes convenience and mobility. Using cloud resources allows avoiding significant costs for equipment and maintenance of own infrastructure, in particular, for small companies and startups. Cloud services are easily scalable, allowing users to increase their resources as needed. Many cloud solutions are automatically updated and maintained, reducing the need for manual work. In addition, most cloud services provide the ability to automatically backup and restore data, which helps to avoid data loss. Disadvantages include data privacy and security, dependence on the Internet connection, denial of control, configuration restrictions, and regulatory compliance issues. Under the terms of cloud computing, user data is stored on third-party servers. This increases the risk of privacy violations and the possibility of unauthorised access. Cloud services require a stable internet connection, and losing Internet access can lead to data unavailability. Using cloud solutions means that users transfer some control over their infrastructure and security to third parties. Some cloud services may limit the user's ability to configure computing resources, and using cloud services may require compliance with various regulatory requirements that are quite complex to meet.

There are many examples of modern cloud computing. For example, AWS, which is one of the leading cloud service providers and offers a wide range of services such as computing, data storage, databases, networks, etc. AWS Lambda allows developers to execute code without the need for infrastructure management. In addition, GCP, another leading cloud service provider, offers a variety of services for developing, deploying, and managing applications in the cloud. And GCP Cloud Functions allows developers to create features that automatically respond to events and requests. In turn, Microsoft Azure is another popular cloud solution that provides a wide range of services for developing, deploying, and managing applications in the cloud. Azure IoT Hub allows a user to connect, monitor, and manage IoT devices. Another example is Salesforce, which is a leading provider of cloud-based customer relationship management (CRM) systems and other CRM services. There are other cloud platforms, but all of them provide a variety of solutions for sales, marketing, customer service, and other business processes. A comparison of these cloud platforms is shown in Table 1.

Table 1. Comparison of leading cloud environments

Platform	Basic services	Advantages	Disadvantages
AWS	Computing, data storage, databases, networks, etc.	Easy access to resources, wide range of services, scalability, automation, backup	High costs, difficulty in using for beginners, low customer support
GCP	Development, deployment, and management of applications in the cloud	Ability to automatically respond to events, wide range of services, scalability	Specificity for use in some other areas, lack of certain services, insufficient data localisation
Microsoft Azure	Development, deployment, and management of applications in the cloud	Wide range of services, scalability, IoT support	Difficult integration with some applications, limited opportunities for users with non-paid support
Salesforce	CRM systems and CRM services	Specialised services for businesses	Limited opportunities for other types of services, high usage costs for some businesses

Source: compiled by the author based on L. Dignan (2021)

Therefore, each cloud platform has its own advantages and disadvantages. When choosing a specific platform to use, an organisation should carefully consider its needs and requirements. It is important to consider which services and functionality are critical for a particular business or project, and what limitations or disadvantages may arise when using a particular platform. Careful planning, risk assessment, and continuous monitoring will help ensure successful use of cloud computing in the enterprise. Despite the presence of many criteria for choosing cloud systems, the main priority will always be security. Thus, the study considers an example of a console programme for security monitoring. The main idea of the code is to analyse event logs and check access to resources to detect suspicious activity (Fig. 1).

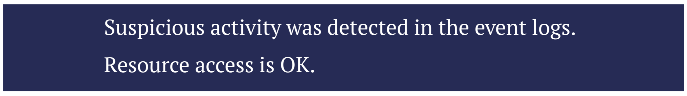
```
import java.util.Timer;
import java.util.TimerTask;
public class SecurityMonitoringSystem {
    public static void main(String[] args) {
        // Analysis of event logs
        boolean eventLogsResult = analyzeEventLogs();
        // Checking access to resources
        boolean resourceAccessResult = checkResourceAccess();
        if (eventLogsResult) {
            System.out.println("Suspicious activity was detected in the event logs.");
        } else {
            System.out.println("The event logs contain no suspicious activity.");
        }
        if (resourceAccessResult) {
            System.out.println("Resource access is OK.");
        } else {
            System.out.println("Incorrect access to resources was detected.");
        }
    }
    // A method for analysing event logs
    private static boolean analyzeEventLogs() {
        int failedLoginAttempts = getFailedLoginAttemptsFromLogs();
        // If the number of failed login attempts exceeds 5, return true (suspicious activity)
        if (failedLoginAttempts > 5) {
            return true;
        }
        // Otherwise, return false (no suspicious activity detected)
        return false;
    }
    // A method for checking access to resources
    private static boolean checkResourceAccess() {
        boolean hasAccessToFile = checkFileAccess("importantfile.txt");
        // If the user has access to the file, return true (access is OK)
        if (hasAccessToFile) {
            return true;
        }
        // Otherwise, return false (incorrect access)
        return false;
    }
    // A function to get the number of failed login attempts from the event logs
    private static int getFailedLoginAttemptsFromLogs() {
        return 7; // An example of a value that can be retrieved from logs
    }
    // A function to check access to a file
    private static boolean checkFileAccess(String fileName) {
        // A function that checks whether a user has access to a file by name
        if (isUserAuthorizedToAccessFile(fileName)) {
            return true; // If the user has access, return true
        } else {
            return false; // If access is not available, return false
        }
    }
    // A function to check user authorization
    private static boolean isUserAuthorizedToAccessFile(String fileName) {
        return true; // In this example, always return true
    }
}
```

Figure 1. Console programme code for security monitoring

Source: created by the author

Firstly, the "main" method is started, which is the starting point of the program. The analyzeEventLogs method analyses event logs. The number of failed login attempts is obtained (the failedLoginAttempts variable), and if this number exceeds, for example, 5, true is set, indicating that suspicious activity has been detected. The checkResourceAccess method checks access to resources. This example checks access to the "importantfile.txt". If the user has access to the file (the hasAccessToFile variable), true is set, indicating correct access. The "main" method displays the results of analysing event logs and checking access to resources on the console.

The programme itself will display the following result (Fig. 2). However, this programme is a basic example and does not include real-world event log analysis or access verification. In a real system, a user will need to implement this functionality using more complex logic and real data.



```
Suspicious activity was detected in the event logs.
Resource access is OK.
```

Figure 2. Programme result

Source: created by the author

Considering the above information, methods for ensuring privacy and security in cloud computing should be developed. These may include the following aspects: data encryption (development of encryption methods to protect data during transmission and storage in cloud computing); authentication and authorisation (implementation of user authentication methods and resource access control); intrusion detection and incident response (development of systems for detecting and responding to suspicious activity or potential intrusions); regulatory requirements and standards (consideration of legislation and standards on data security and privacy); integration with modern applications (development of methods for secure integration of cloud computing with modern applications); monitoring and logging (implementation of monitoring and event logging systems to track activity and detect suspicious activity); user identification and authentication (development of methods for securely identifying and authenticating users before granting access to resources).

Therefore, due to the constant development of cryptographic methods, it is recommended to follow the latest trends and adapt encryption to new challenges. It is important to study modern approaches to multi-level authentication and role-based access control. A combination of monitoring techniques and intelligent analytics can be useful. It is recommended to constantly update the knowledge of security legislation and standards. Logging techniques and monitoring systems should be developed to detect problems in a timely manner. The general recommendation is to be constantly open to new security techniques and technologies in cloud computing and actively participate in the community to share knowledge and improve security practices. A block diagram of these security methods in cloud computing is shown in Figure 3.

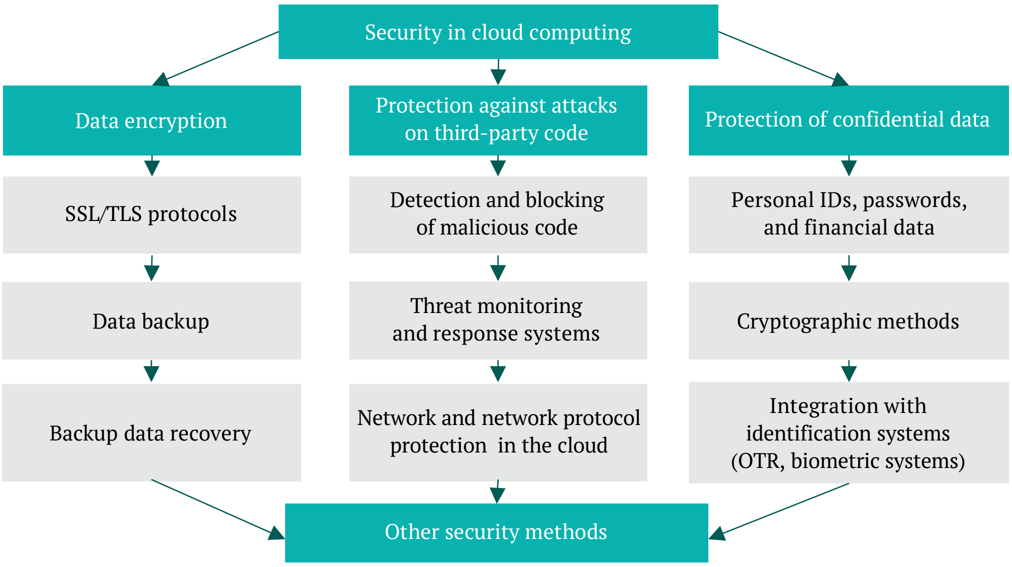

Security in cloud computing
Data encryption
Protection against attacks on third-party code
Protection of confidential data
SSL/TLS protocols
Detection and blocking of malicious code
Personal IDs, passwords, and financial data
Data backup
Threat monitoring and response systems
Cryptographic methods
Backup data recovery
Network and network protocol protection in the cloud
Integration with identification systems (OTR, biometric systems)
Other security methods

Figure 3. Provision of security in cloud computing

Note: SSL – secure sockets layer; TLS – transport layer security; OTR – off-the-record messaging

Source: created by the author

This diagram reflects a group of security techniques that can be used to ensure privacy and security in cloud environments. Each method has its own sub-branch and includes different approaches and technologies to ensure the relevant aspects of security and privacy. Based on the conducted research, certain recommendations are proposed that follow from the study and have important practical significance. It is necessary to ensure the security of data at every stage of its life cycle, from storage and transmission to processing. It is recommended to use data encryption and improve user authorisation and authentication methods. Regular security audits and activity monitoring should be conducted to detect suspicious activity. This will help to identify possible threats in time and take measures to prevent them. It is worth developing plans for responding to possible security incidents and backing up data. Inventory and plans will help restore the system after the incident and reduce possible losses. It is important to learn about and comply with all regulatory requirements and standards relating to data processing and storage. This will help to avoid legal problems and fines. Consideration should also be given to introducing innovative security approaches and technologies, such as AI and machine learning, to detect threats. Provide training and advanced training of security personnel. An informed workforce is an important link in ensuring security in cloud computing, and it is necessary to cooperate with cloud service providers and demand high security standards from them. Check their certificates and security recommendations. These guidelines are aimed at improving security and privacy in cloud systems and can help organisations and users store and process data in a secure environment.

Therefore, the results show that security can be achieved in cloud environments if appropriate measures and methods are taken. The developed methods and approaches play an important role in ensuring data confidentiality and protecting resources. These results can open up prospects for the development and improvement of security systems in cloud computing.

DISCUSSION

There are various studies on security in cloud computing. Some researchers focus on aspects of data encryption during transmission and storage, while others focus on user authentication and access control, and explore aspects of intrusion detection and monitoring systems. It is worth considering the study by S. Varun (2023), which provides an overview of security and privacy issues in cloud computing and proposed solutions. The researcher notes that cloud computing has become an important part of modern business, but at the same time there are significant threats to data security and privacy. Various aspects of security and privacy, such as encryption, access control, and identity management, are addressed, and the role of cloud service providers is considered. In conclusion, the paper provides recommendations for improving the level of security and privacy in cloud computing. Common aspects between this and the current study are the creation of solutions for implementing privacy and security in cloud computing, and in the aspects of security and privacy. However, in the first case, the research is more theoretical, while this study contains a practical implementation of the subject.

I.S. Mohd Fadhil *et al*. (2023) emphasise that cloud computing is an important technology that provides access to computing resources over the Internet. The paper examines the security and privacy challenges in cloud computing that arise with the widespread use of this technology. The researchers analyse methods to ensure data privacy, and discuss the role of cloud service providers and compliance issues. In conclusion, they make recommendations for improving security and privacy in cloud computing. Both studies applied practices for security and privacy issues in cloud computing, and considered examples of various cloud services. However, the examples themselves and their descriptions differ.

The study by R. Patel *et al*. (2023) also points out that when an organisation moves to cloud computing to reduce costs and improve efficiency, privacy concerns arise. The researchers emphasise that in order to effectively implement privacy protection strategies in cloud computing, modern methods for managing these problems are required. The paper discusses the needs for protecting private data, and considers the basic principles of security measures in cloud computing. The comparison then discusses various privacy strategies in cloud environments. As in this study, it introduces certain methods of providing security in cloud computing, but these methods are different. F.K. Aljwari (2023) notes that cloud computing is a fast-growing field in the field of information technology. They allow accessing various tools and services over the network. However, there are serious issues with data privacy and security. The paper discusses these issues and possible solutions that are relevant for researchers and security experts. Common aspects between the two studies are security issues in cloud computing. But this study focuses specifically on creating methods for ensuring privacy and security, and the rest – on ways to solve problems on this topic.

J. Uma Maheswari *et al*. (2023) also emphasise that the modern world is increasingly using cloud computing, which allows organising data, managing its storage, processing and access. However, this technology raises questions about the security and privacy of data in cloud environments. The main task of using cloud computing is to keep data private and secure when processing and storing it in external data centres. This study discusses various risks, including internal threats, data leaks, and illegal access to sensitive information. Legal and standard requirements for protecting user data in cloud environments are also considered. Both studies focus on security and privacy in cloud systems, but the current study does not address specific standard and legal protection requirements, unlike the study analysed.

In turn, A. Bhansali (2023) points out that there are many risks that threaten the privacy and security of the Internet environment. Therefore, the researcher discusses these issues and possible solutions. The most common user complaint about cloud computing is the security and privacy of data in the cloud. The researcher discusses in detail issues related to internal threats, data leaks, and illegal access to confidential information. Ultimately, the paper highlights the legal requirements that businesses must comply with to protect user data in the cloud. Thus, privacy and security issues in cloud computing remain relevant for organisations and individuals. Both studies address security threats in the cloud environment. However, the current study is not as focused on legal requirements as another.

N. Ukeje *et al*. (2024) emphasise that many companies use cloud services to store data in a virtual environment. However, there are problems with ensuring the security and privacy of data in cloud computing, as users do not have control over what happens in the cloud, and this poses threats to the security and privacy of information. The study discusses issues related to data security and privacy in cloud computing and how to solve them. The main solution to this problem is the preferred reporting items for systematic reviews and meta-analyses (PRISMA) approach. It can be concluded that both studies focus on the issues of data protection and privacy in cloud computing. However, the current study develops specific security and privacy techniques, while another uses a specific PRISMA approach.

Just like the previous researchers, S. Reema (2023) notes that the proliferation of cloud computing has raised serious questions about the security and privacy of sensitive information stored in the cloud. The purpose of the study is to explore the security and privacy issues associated with cloud computing and consider the possibilities of using this technology to solve them. The paper emphasises that cloud computing can be an effective solution to security and privacy issues, provided that relevant standards and practices are followed. Therefore, the general criteria are to consider security and privacy in the cloud environment. Although, this study is more practical, since it contains code and a block diagram. And the considered study is more theoretical, since it contains an analysis of ways to achieve security and privacy.

N. Haider & C. Azad (2022) considers "Fog computing", which aims to bring the cloud closer to IoT devices to solve the problems that arise in cloud computing when processing IoT data. This is an intermediate layer between the cloud and computers. In addition to the security and privacy issues that are inherent in cloud computing, Fog computing also has its own set of unique issues. The study analyses previous studies of Fog computing applications to identify security flaws. It evaluates the impact of these problems and possible solutions, provides guidance on future security for those responsible for the development and design of Fog systems. What the two studies have in common is the use of cloud technologies and the identification of related problems. Despite this, the 2022 paper deals specifically with Fog computing and the IoT system, which is not present in this study.

Other studies also use cloud computing, examining privacy and security issues and how to address them. For example, E. Geetha Rani & D.T. Chetana (2023) note that the widespread use of cloud computing has raised serious questions about the security and privacy of information stored in the cloud. The study examines various security and privacy issues related to cloud computing and examines how the technology can be used to address these issues. The researchers suggest that by following certain best practices on the part of cloud service providers and users, cloud computing can be an effective solution to security and privacy concerns in the digital age.

The purpose of the study by Y. Abdulsalam & M. Hedabou (2022) is to examine the security and privacy challenges associated with cloud computing and examine the technology's capabilities to overcome these challenges. By analysing existing research and examining practical examples, the paper suggests that cloud computing can be an effective solution to security and privacy concerns in the digital age, provided that certain best practices are followed by both cloud service providers and users. H. Gavit & Y. Patil (2023) note that cloud computing has gained popularity due to its profitability and flexibility. However, security remains a serious issue, as data in the cloud can be vulnerable to breaches, internal threats, and other risks. The study examines security issues and suggests measures to address them. Important security measures that organisations need to implement include encryption, access control, multi-factor authentication, audits, backups, secure configuration, security testing, incident response plans, etc. The implementation of these measures will allow taking advantage of cloud computing, ensuring the security and confidentiality of data. M.Z. Hasan *et al*. (2023) explores various security issues in cloud computing and measures that can be taken to address them. The study discusses data security and integrity, which are key aspects. The researchers emphasise that organisations should develop a comprehensive security strategy that considers the specific needs and requirements of their cloud resources to ensure the security and confidentiality of their data and applications.

It can be concluded that all considered studies are aimed at developing ways and solving problems related to user privacy and security in cloud computing. This paper also addresses these aspects, but it offers a comprehensive approach to the problem, providing not only an analysis of existing risks and challenges, but also considering practical recommendations for implementing effective security and privacy strategies in cloud computing. In addition, this study provides promising guidance for the development of this area, contributing to further improvements in data protection and security in cloud computing.

CONCLUSIONS

This study considered various aspects of security and privacy in cloud computing. The possibilities of integrating security at various stages of software development for consistent and effective implementation of security controls in cloud systems are examined. The findings of the study include a number of solutions. The main result is the development of security monitoring application that analyses event logs and checks access to resources. It shows whether suspicious activity has been detected and can be a basis for practical application. A comparison table of various cloud platforms has been compiled, with an emphasis on their advantages and disadvantages in the context of data protection and privacy. For this purpose, some well-known cloud services were analysed. A block diagram has been developed for security methods in cloud computing, which illustrates the relationship between various aspects of security in cloud systems. This diagram covers information encoding, protection from external attacks, and security of private data. The results also include analysis of various aspects of security and privacy practices in cloud computing, such as authorisation, data encryption, intrusion detection, regulatory compliance, logging, integration with modern applications, monitoring, and user authentication and identification.

The development and application of new cryptographic protocols can help improve the level of security in cloud environments. For practical applications, it is recommended to implement systems for monitoring and responding to suspicious activity, which would allow organisations to maintain a stable state of security and provide an appropriate response to possible threats. Security should also be considered as an ongoing process and security practices should be updated based on new threats and vulnerabilities. Ensuring privacy and security in cloud computing requires a systematic approach. In further research, it is advisable to continue developing innovative methods and approaches to ensuring security in cloud computing. This will help increase user confidence in cloud technologies and help meet regulatory requirements for data processing.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abdulsalam, Y., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. *Future Internet*, 14(1), article number 11. doi: 10.3390/fi14010011.

[2] Aljwari, F.K. (2023). Privacy and security in cloud-based computing: Challenges and solutions. In X. Wang (Ed.), *Research and applications towards mathematics and computer science* (Vol. 2; pp. 1-15). Kolkata: B.P. International. doi: 10.9734/bpi/ratmcs/v2/19324D.

[3] Amro, T. (2022). The connection of the system for ensuring information security and public administration under the conditions of war-time: Methods and possibilities. *Public Management*, 5(33), 83-88. doi: 10.32689/2617-2224-2022-5(33)-11.

[4] Bhansali, A. (2023). Cloud security and privacy. *International Journal for Research in Applied Science and Engineering Technology*, 11(8), 1539-1542. doi: 10.22214/ijraset.2023.55416.

[5] Bohomia, V.I., & Kochegarov, V.S. (2023). Cybersecurity in cloud services using cryptographic methods. *Water Transport*, 1(37), 239-246. doi: 10.33298/2226-8553.2023.1.37.27.

[6] Dignan, L. (2021). *Top cloud providers: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players*. Retrieved from https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/.

[7] Gavit, H., & Patil, Y. (2023). *Enhancing security in cloud computing*. Retrieved from https://www.researchgate.net/publication/371574904_Enhancing_Security_in_cloud_computing.

[8] Geetha Rani, E., & Chetana, D.T. (2023). A survey of recent cloud computing data security and privacy disputes and defending strategies. In J.C. Bansal, H. Sharma & A. Chakravorty (Eds.), *Congress on smart computing technologies. CSCT 2022. Smart innovation, systems and technologies* (Vol. 351; pp. 407-418). Singapore: Springer. doi: 10.1007/978-981-99-2468-4_31.

[9] Haider, N., & Azad, C. (2022). Data security and privacy in fog computing applications. In P. Bhambri, S. Rani, G. Gupta & A. Khang (Eds.), *Cloud and fog computing platforms for internet of things* (pp. 57-67). New York: Chapman and Hall/CRC.

[10] Hasan, M.Z., Hussain, M.Z., Mubarak, Z., Siddiqui, A.A., Qureshi, A.M., & Ismail, I. (2023). Data security and integrity in cloud computing. In *2023 international conference for advancement in technology (ICONAT)* (pp. 1-5). Goa: IEEE. doi: 10.1109/ICONAT57137.2023.10080440.

[11] Horodyskyi, M., Polishchuk, I., & Yakimtseva, Yu. (2021). Methods of development and use of cloud technologies in accounting. *Economics, Management and Administration*, 2(96), 37-46. doi: 10.26642/ema-2021-2(96)-37-46.

[12] Mazur, V. (2023). *Security assessment of using cloud technologies and development of methods for protection against cyber-attacks on cloud services*. (Bachelor thesis, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine).

[13] Mohd Fadhil, I.S., Mohd Nizar, N.B., & Rostam, R.J. (2023). Security and privacy issues in cloud computing. *TechRxiv*. doi: 10.36227/techrxiv.23506905.v1.

[14] Nafiiev, A., & Lande, D. (2023). Malware detection model based on machine learning. *Bulletin of Cherkasy State Technological University*, 3, 40-50. doi: 10.24025/2306-4412.3.2023.286374.

[15] Patel, R.K., Gidwani, P., & Patel, N.R. (2023). Privacy preservation and cloud computing. In D. Lakshmi & A.K. Tyagi (Eds.), *Privacy preservation and secured data storage in cloud computing* (pp. 88-107). Hershey: IGI Global. doi: 10.4018/979-8-3693-0593-5.ch004.

[16] Reema, S. (2023). Cloud computing as a solution for security and privacy concerns. *International Journal for Research in Applied Science and Engineering Technology*, 11(3), 183-187. doi: 10.22214/ijraset.2023.49375.

[17] Sultanova, L., & Prokofieva, M. (2022). Digital security in higher education. *Adult Education: Theory, Experience, Prospects*, 21(1), 106-117. doi: 10.35387/od.1(21).2022.106-117.

[18] Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*. doi: 10.1007/s10207-023-00797-6.

[19] Uma Maheswari, J., Vijayalakshmi, S., Rajiv Gandhi, N., Alzubaidi, L.H., Khonimkulov, A., & Elangovan, R. (2023). Data privacy and security in cloud computing environments. *E3S Web of Conferences*, 399, article number 04040. doi: 10.1051/e3sconf/202339904040.

[20] Vakhula, O., & Opirskyy, I. (2023). Research on security issues in cloud environments and solutions using the “security as code” approach. *Ukrainian Information Security Research Journal*, 25(3), 113-122. doi: 10.18372/2410-7840.25.17936.

[21] Varun, S. (2023). Security and privacy in cloud computing: Challenges and solutions. *International Scientific Journal of Engineering and Management*, 2(4). doi: 10.55041/ISJEM00304.

Безпека в хмарних обчисленнях: методи забезпечення приватності та інтеграції в сучасних додатках

Олексій Геннадійович Зарічук

Менеджер комп'ютерних та інформаційних систем
ТОВ «Фідес»
02000, вул. Є. Сверстюка, 11А, м. Київ, Україна
https://orcid.org/0009-0009-0771-8465

Анотація. Хмарні обчислення стали необхідною складовою для зберігання й обробки даних та набувають все більшого поширення. Проте існують загрози щодо безпеки й приватності даних користувачів, через що важливо з'ясувати найефективніші методи забезпечення безпеки даних у хмарі. Мета дослідження полягала в розробці методів, спрямованих на забезпечення конфіденційності та безпеки в хмарних середовищах і в сучасних застосунках. Використано метод аналізу для розгляду й вивчення інших публікацій із теми, а також метод експерименту для практичної реалізації. Основні результати дослідження включають у себе написання програми моніторингу безпеки. Вона аналізує журнали подій та визначає кількість невдалих спроб входу, що показує виявлення чи відсутність підозрілої активності. Проводиться перевірка доступу до ресурсів, необхідна інформація виводиться на консоль. Створено таблицю порівняння хмарних платформ, з урахуванням їх переваг та недоліків у контексті безпеки та конфіденційності даних. У ній вказуються критерії постачання послуг обраних сервісів. Сформовано структурну схему способів забезпечення захисту в хмарних обчисленнях, що ілюструє взаємозв'язок між різними аспектами забезпечення захисту в хмарних системах. Вона містить параметри та стратегії щодо шифрування даних, захисту конфіденційних даних та протидії атакам. Розглянуто різні аспекти безпеки та методи забезпечення конфіденційності в хмарних обчисленнях, а саме: авторизацію, виявлення вторгнень, регуляторні вимоги, інтеграцію з сучасними додатками, моніторинг і журналювання, ідентифікацію та аутентифікацію користувачів. Практичне значення дослідження полягає в створенні інноваційних способів, які допоможуть підвищити рівень безпеки та приватності в хмарних обчисленнях. Вони дозволять розробникам та адміністраторам хмарних систем ефективно захищати дані користувачів і забезпечувати їхню конфіденційність у сучасних додатках

Ключові слова: онлайн-розрахунки; захист даних; гарантування конфіденційності; охорона актуальних застосунків; віртуальне середовище