BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en Vol. 29 No. 3. 2024

UDC 004.056.55:004.75
DOI: 10.62660/bcstu/3.2024.31

Data encryption as a method of protecting personal data in a cloud environment

Samur Ahmadov*
Postgraduate Student
Azerbaijan Technical University
AZ1073, 25 Huseyn Cavid Ave., Baku, Azerbaijan
https://orcid.org/0000-0003-0733-898X

Abstract. In the context of cloud technologies, encryption plays a critical role, as data are constantly transmitted over the network and stored on remote servers, which makes them a potential target for cyber-attacks. The purpose of the study lied in a comprehensive analysis of data encryption methods as the main tool for protecting personal information in cloud services. Modern encryption technologies, including symmetric and asymmetric encryption, and their application in various cloud platforms were considered. A comparative analysis of these methods was conducted in terms of their effectiveness, impact on system performance, and complexity in implementation. An important aspect of the study was the examination of problems related to the management of encryption keys, including their secure storage and protection from unauthorised access. The study also examined examples of successful encryption implementation on popular cloud platforms and ways to ensure their compliance with the requirements of legislation in the field of personal data protection. The regulatory acts regulating the processing and storage of personal information and their impact on the choice and implementation of encryption methods in the cloud were analysed. The results of the study showed that encryption remains one of the most reliable ways to protect data in a cloud environment but an integrated approach is needed for its effective application. Optimal data protection includes not only encryption but also key management, regular security monitoring, and staff training. This helps minimise the risks of data leaks and increase user confidence in cloud services

Keywords: key management; system performance; information security; information leaks; confidentiality

INTRODUCTION

With the rapid development of information technology and an increase in the volume of data transmitted and stored in cloud services, personal data protection has become one of the most important tasks for organisations at all levels. Many companies face cyber-attacks, and many of them recognise that the leakage of personal data can substantially damage their reputation and financial position. In this regard, data encryption seems to be a critical tool for ensuring the confidentiality and security of personal information.

The relevance of the topic of data encryption in the cloud environment is due not only to an increase in the number of cyber-attacks but also to changes in legislation requiring organisations to strictly comply with personal data protection standards. Failure to comply with these requirements can lead to serious fines and loss of trust on the part of users. In the context of globalisation and an increasing number of international transactions, companies are faced with the need to comply with various legal norms, which complicates the process of data protection.

Article's History: Received 23.06.2024; Revised 05.09.2024; Accepted 21.10.2024

Suggested Citation:
Ahmadov, S. (2024). Data encryption as a method of protecting personal data in a cloud environment. *Bulletin of Cherkasy State Technological University*, 29(3), 31-41. doi: 10.62660/bcstu/3.2024.34.

*Corresponding author

The problem of data encryption lies not only in its implementation but also in the need to ensure a balance between security and system performance. The use of complex encryption algorithms can negatively affect the performance of cloud services, which requires developers to find optimal solutions. In addition, many organisations face a lack of knowledge and resources to properly implement encryption, which leads to vulnerabilities in their information systems.

The basics of data encryption cover a variety of methods and algorithms used to protect information. These methods allow converting data into an unreadable format that can only be decrypted using the appropriate keys. However, despite its advantages, encryption is not a universal solution; it must be integrated into an overall data security strategy that includes authentication, access control, and regular audits.

Data encryption in a cloud environment allows identifying several critical studies that contribute to understanding the issues of personal data protection. H. Abroshan (2021) investigated the impact of encryption on the performance of cloud services and concluded that the use of encryption algorithms can lead to a noticeable increase in request processing time. The author suggested balancing the level of security and performance, which is critical for the successful implementation of encryption. M. Zeng *et al*. (2019) focused on the importance of asymmetric encryption in cloud applications. They showed that this methodology provides a high level of security when exchanging data between users and cloud providers, reducing the risk of information interception. B. Custers *et al*. (2019), in turn, described approaches to integrating data encryption into an access control system. They noted that the use of encryption in combination with reliable authentication substantially increases the level of protection of personal data. V. Rudnytsky *et al*. (2022) also conducted a review of modern encryption algorithms and offered a comparative analysis of their effectiveness and security. They determined that some new algorithms provide a higher level of protection at a lower cost of resources. M.N. Asghar *et al*. (2019) investigated the problems associated with the legislative regulation of data encryption. They argued that many companies do not comply with the requirements of the General Data Protection Regulation (GDPR) (2016) due to the lack of clear guidance on the use of encryption.

H. Malvai *et al*. (2023) drew attention to the need to ensure transparency in encryption processes. They argued that users should be aware of how their data is encrypted and stored to build trust in cloud providers. D.K.R. Shukla *et al*. (2021), in turn, analysed the practical aspects of implementing encryption in cloud services. Their results showed that best practices include regular updating of encryption keys and the use of multi-factor authentication. K.R. Sajay *et al*. (2019) focused on comparing different encryption protocols for data transmission over cloud services. Their paper has established that using Secure Sockets Layer or Transport Layer Security is the most secure solution to protect data during transmission. T. Palit *et al*. (2019) investigated the role of encryption in protecting data from internal threats. They argued that data encryption at the storage level is an important measure against leaks related to the actions of unscrupulous employees. A. Calder & S. Watkins (2024) emphasised the need for a comprehensive approach to data security, including both technical and organisational measures.

An analysis of the papers of these authors shows that data encryption is a multifaceted topic that requires an integrated approach. Despite a substantial amount of research in the field of data encryption in the cloud environment, there are still subjects that are insufficiently examined or require more in-depth study. One of these subjects is the optimisation of encryption algorithms to improve performance while maintaining a high level of security. In addition, the issues of encryption key management in multi-cloud environments and the problems of compliance with international norms and standards when working with personal data on a global scale remain insufficiently investigated. The purpose of the study was to explore the best approaches to using data encryption in a cloud environment, considering the need to improve performance and comply with international security standards. The objectives of the study were to analyse modern encryption algorithms in terms of their performance and security in cloud services and analyse existing encryption key management methods and their applicability in multi-cloud environments.

MATERIALS AND METHODS

In this study, various encryption methods and algorithms were used to protect both personal and corporate information and to comply with GDPR requirements. Countries that have implemented regulations similar to the EU GDPR were selected for the study. The main objects of the analysis were the legal systems of Argentina, Japan, Brazil, Canada, and South Korea, which have implemented data protection laws (Data privacy laws…, 2024).

The materials for the study were the texts of these legislative acts, and documents of the European Commission establishing criteria for assessing the adequacy of data protection. The methodology included comparative legal analysis, classification of requirements, and identification of differences in the regulation of personal data processing and protection. Indicators such as user information requirements, data processing consent management, data subjects' rights and information security mechanisms were used for the analysis. The first stage of this study was the selection of suitable encryption algorithms. Various methods have been examined that have a high degree of safety and are used

in real conditions to do this. During the selection process, special attention was paid to algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). AES, which is a symmetric algorithm, has proven itself to be a high-performance and reliable tool widely used in commercial applications. RSA, being an asymmetric method, plays an important role in the secure transfer of keys and digital signatures, which makes it indispensable in data protection conditions.

Three cloud platforms were considered for the study: Amazon Web Services (2024) (AWS), Microsoft Azure (Azure encryption overview, 2024), and Google Cloud Platform (GCP) (Key purposes and..., 2024). Each of them implements both symmetric and asymmetric encryption mechanisms to protect data. AWS used Amazon S3 Server-Side Encryption (SSE) and AWS Key Management Service (KMS), which use AES-256 to encrypt data. In Microsoft Azure, the Azure Storage Service Encryption system and Azure Key Vault for key management were analysed. GCP explored Google Cloud KMS for symmetric encryption and support for asymmetric methods for secure key transfer.

The next important step was to study the encryption keys, which is a critical aspect of data protection. Both static and dynamic keys were investigated. Static keys ensure consistency throughout the lifetime, while dynamic keys are created for each session, which substantially reduces the risk of compromise. Various metrics were examined to analyse the performance of the encryption algorithms used. Primarily, this is the encryption and decryption time, which allows understanding how fast algorithms can process data. In addition, a security assessment was conducted based on known vulnerabilities and attack resistance. Equally important was the examination of the use of resources, such as RAM and processor time, in the process of performing encryption operations.

At the final stage of the study, a comparative analysis of the data was conducted. This allows not only to compare the execution time of various algorithms but also to assess their safety based on theoretical and practical scenarios. As a result of the analysis, it became clear that the choice of encryption methods, algorithms and approaches to key generation and management directly affects the level of protection of personal information. The correct application of these technologies not only contributes to compliance with GDPR requirements but also ensures a high level of security in conditions of a constant increase in the volume of processed data.

RESULTS

Data encryption plays a critical role in modern digital security. The volume of processed and stored data is growing every year, which makes the need to protect personal and corporate information more urgent. Encryption is the process of converting information into an unreadable format to protect against unauthorised access. In addition to its technical significance, encryption also complies with modern regulatory requirements such as GDPR.

The main purpose of encryption is to ensure data confidentiality. This means that only authorised users can access encrypted information. In addition, encryption guarantees the integrity of the data, preventing it from being altered or corrupted during transmission. In modern conditions, encryption also helps companies comply with regulatory requirements, which is especially important for protecting users' personal information. GDPR, for example, is an EU regulation adopted on April 14, 2016, and introduced on May 25, 2018, to protect the personal data of EU citizens, regardless of where they are processed.

Data encryption is an important element of protecting both personal and corporate information, preventing data leaks and theft. The encryption process involves choosing an algorithm that converts the source data into an encrypted format using a key. The encryption algorithm and the key work together to make the data unreadable to unauthorised persons. This process includes several stages, starting with the selection of an algorithm and ending with the generation of an encryption key. Some algorithms provide static keys, while others are dynamically updated in each session (Rafique *et al.*, 2021).

There are two main types of encryptions: symmetric and asymmetric. Symmetric encryption uses a single key for both encryption and decryption of data. This is faster and requires fewer resources compared to asymmetric encryption, but requires secure key transfer between the parties, which is its weak point. Asymmetric encryption, on the other hand, uses a key pair: public and private. The public key is used to encrypt data and the private key is used to decrypt it, which provides a higher level of security, although the process is slower (Marqas *et al.*, 2020). Table 1 shows a comparison of symmetric and asymmetric encryption.

Table 1. Comparison of symmetric and asymmetric encryption

Characteristics	Symmetric encryption	Asymmetric encryption
Using keys	The same key is used for encryption and decryption. Both the sender and the recipient must own this key	The encryption uses a public key that is accessible to everyone. For decryption – a private key known only to the recipient
Key transfer	It is necessary to securely transfer the key from the sender to the recipient to successfully exchange information. The security of key transfer is the weak point of the method	The public key can be opened and transferred without risk. Only the private key should be kept secret, which makes key transfer more secure

Continued Table 1.

Characteristics	Symmetric encryption	Asymmetric encryption
Efficiency	Encryption is fast and requires less computing resources, which makes it more efficient to work with large amounts of data	Encryption is slower and requires more computing resources, especially at the decryption stage. Suitable for smaller amounts of data and more sensitive operations
Usage examples	It is used for encrypting files, databases, data transmission over the network, and other situations where fast processing and encryption of large amounts of data is required. For example, to encrypt file systems or stream data	It is used to protect key exchange, digital signatures, and data in e-mail, online transactions and other cases where the secure transfer of confidential information is required. For example, to securely exchange symmetric encryption keys over the Internet
Key security	The main threat is the interception of the key since its knowledge gives the attacker the opportunity to decrypt all data	The public key is accessible to everyone, and even if it is intercepted, an attacker will not be able to decrypt the data without the private key. The private key is protected and must remain secret
Algorithms	Examples: AES, Data Encryption Standard	Examples: RSA, Elliptic Curve Cryptography
Visual concept	Visually, the symmetric encryption process can be represented as the interaction of two parties (sender and recipient) who use the same key to encrypt and decrypt messages. Both participants must agree on this key in advance, and it must remain secret from outsiders	Visually, asymmetric encryption can be depicted as a process in which the sender encrypts a message using a public key (which is available to everyone), and the recipient decrypts it using a private key that is kept secret. Thus, the security of key transfer is not violated
Combination of methods	It is used in combination with asymmetric encryption to encrypt large amounts of data after secure key exchange through asymmetric methods	It is used for the initial secure exchange of symmetric encryption keys, which allows using faster symmetric algorithms for data transmission in the future

Source: compiled by the author

Symmetric and asymmetric encryption are widely used on various cloud platforms to protect data during storage and transmission. In AWS, symmetric encryption is implemented through Amazon S3 SSE and AWS KMS, which use AES-256 to quickly encrypt large amounts of data, while asymmetric encryption is used for key management and digital signatures. In Microsoft Azure, symmetric encryption is provided using Azure Storage Service Encryption, which automatically encrypts data, and for asymmetric encryption, Azure Key Vault is used to manage SSL/TLS certificates. On GCP, data is automatically encrypted with symmetric algorithms such as AES-256 via Google Cloud KMS and asymmetric encryption is supported for secure key transfer and digital signatures. Thus, symmetric encryption provides high performance for encrypting large amounts of data, while asymmetric encryption is used for specialised tasks such as secure key transfer and digital signatures.

Symmetric encryption is especially popular due to its simplicity and speed. It is often used in systems where fast data processing is required, such as databases and cloud systems. Algorithms like AES provide reliable encryption that requires minimal computing resources, which makes them attractive for large amounts of data. However, symmetric encryption has its drawbacks, including the need to securely transfer the secret key, which can be a problem when working with multiple users (Gui *et al.*, 2023). In large organisations, key management becomes a complex task that requires regular updating and key protection.

Symmetric encryption, although it is an effective and fast method of data protection, is not without drawbacks. One of the main problems of this approach is the need to securely transfer the secret key between the participants. If the key falls into the hands of intruders, they will be able to decrypt all encrypted data. This makes the key exchange process vulnerable and requires the use of additional security measures, such as secure data channels. Also, key management in large organisations can be difficult, especially when it requires regular key updates for multiple users, which increases the risk of leakage (Li *et al.*, 2019).

Asymmetric encryption is a more complex but secure encryption method. Its key feature is that the public key can be freely distributed, and the private key is kept secret. This solves the problem of secure key transfer since the public key can be accessed by any user who wishes to send an encrypted message without worrying about its transmission through secure channels. However, asymmetric encryption requires more computing resources, which makes it less efficient for large amounts of data. The process of asymmetric encryption begins with the generation of a key pair. The public key can be freely distributed, and the private key is kept by the owner (Senthilkumar & Geetha, 2020). When the sender wants to encrypt a message, they use the recipient's public key. After encryption, the data is

converted into ciphertext and transmitted over any connection, even if it is insecure. Even if an attacker intercept encrypted data, they will not be able to decrypt it without a private key.

The key advantage of asymmetric encryption is its ability to securely transfer keys over open networks. This makes it especially important for applications such as e-commerce, banking transactions, and systems where data must remain confidential. However, the slowness of this method makes it impractical for large amounts of data. One of the main challenges when using encryption is key management. Organisations need to develop reliable systems for creating, storing, transferring, and updating encryption keys. Loss or compromise of the key may result in loss of access to the data or its disclosure. This is especially important for companies that work with confidential information, such as financial data or personal information of users.

It is advisable to consider in more detail the disadvantages of asymmetric encryption. Firstly, it is usually slower than symmetric encryption due to the more complex mathematical operations used in the encryption and decryption process. Additionally, performing asymmetric encryption requires more computing resources, which can be a problem for devices with limited capabilities. Managing key pairs can also be difficult, especially in large organisations where many users interact with each other. Nevertheless, asymmetric encryption is a powerful tool for ensuring data security in modern digital communications. Due to the use of a key pair, it provides reliable information protection and allows authenticating senders. Despite its limitations, asymmetric encryption continues to be an important element in the data security system, especially in the context of cloud technologies and Internet communications. Moreover, asymmetric encryption allows not only to encrypt data but also to verify the identity of the sender. By signing the data with their private key, the sender provides the recipient with the opportunity to verify the authenticity of the data using the public key (Al-Shabi, 2019). This creates an additional level of trust in communications.

With the development of technology, data encryption is becoming more complex and multilevel. Quantum encryption, for example, promises a new level of security that can withstand future threats related to quantum computing. Adaptive algorithms can also change encryption settings depending on the threat level, which will make systems more flexible and secure. However, the implementation of encryption requires substantial infrastructure costs and staff training. This can be a serious challenge for small and medium-sized businesses. However, despite all the difficulties, the correct implementation of data encryption increases customer confidence and reduces the risks of data leakage. Nevertheless, in the future, data encryption will become an integral part of digital security, requiring an integrated approach that will include the introduction of modern technologies and the development of a security culture within organisations. Table 2 shows the advantages and disadvantages of data encryption in a cloud environment.

Table 2. Advantages and disadvantages of data encryption in a cloud environment

Aspect	Advantages	Disadvantages
Data protection	Ensures data privacy even in case of leaks or attacks	Dependence on key management, possible data loss in case of error
Data transmission	Protects data both at rest and when transmitted over the Internet	It may be difficult for authorised users to access the data
Compliance with regulations	Helps to comply with security standards such as GDPR	Requires additional resources to meet all the requirements of the regulations
Efficiency	Cloud providers offer flexible and scalable solutions	Encryption and decryption can slow down applications and systems
Key management	Encryption ensures that data is inaccessible without a key	Key loss can lead to data loss, complexity of key management
Dependence on the provider	Providers offer built-in encryption tools	There is a dependence on cloud services and their security standards
Integration with other systems	Secure data can be used in hybrid cloud environments	Integration between systems can be complicated due to data encryption

Source: compiled by the author

The adoption of the GDPR was an important step in regulating the protection of personal information in the context of the active growth of digital technologies. This regulation established strict requirements for companies and organisations working with personal data and provided users with new rights and opportunities to control their privacy. Personal data such as names, contact information, and financial information have long been an important resource for many companies. With the increasing volume of data and the development of the Internet, it has become clear that stricter control over their use and protection is required. GDPR was designed to regulate these processes and ensure transparency regarding data processing.

Compliance with GDPR requirements has become an important challenge for businesses. Companies are

faced with the need to modernise their data management systems, introduce stricter security methods, and train staff in new rules. This was especially true for organisations that work with large amounts of personal data, for example, in the field of technology, finance, or medicine (Matulevičius *et al.*, 2020). Investments in cybersecurity and compliance with the regulations have become mandatory since serious fines are provided for violations of the GDPR, which can reach large amounts. This motivated companies to review their data protection strategies and take measures to minimise the risks of breaches. However, apart from the costs, compliance with the regulations has also brought positive results for companies. Transparent methods of working with data have increased customer trust, and compliance with high security standards has become a competitive advantage. Many organisations that have adapted to new requirements in time have improved their reputation and strengthened their positions in the market.

Despite the evident advantages, meeting GDPR requirements has proved to be a difficult task for many companies. This was especially true for small and medium-sized businesses, where resources for the implementation of new standards were limited. Many companies are faced with the need to redesign their business processes and adapt their internal infrastructure to ensure compliance with regulations. Compliance with the requirements in the context of globalisation has become especially difficult for businesses. Companies operating internationally had to consider the various laws and requirements of different countries in the field of data protection. This created additional difficulties and required the introduction of complex information management systems. Despite the fact that GDPR is an EU law, its influence has spread to many countries outside Europe. Argentina, Japan, Canada, and New Zealand are recognised by the EU as providing an adequate level of data protection. Countries such as Brazil and South Korea have implemented similar data protection laws, which simplifies cross-border transactions and ensures compliance with high privacy standards. Table 3 describes how countries outside the EU comply with data protection rules similar to GDPR.

Table 3. Countries outside the EU that comply with data protection rules similar to GDPR

Country	Law or Regulation	GDPR compliance	Features
Argentina	Personal Data Protection Law (Act 25.326)	Recognised by the European Commission as a country with adequate protection	The first Latin American country recognised as GDPR compliant
Japan	Act "On the Protection of Personal Information"	Reached an agreement with the EU on the recognition of the level of data protection	Recognised by the European Commission as providing adequate data protection
Canada	Personal Information Protection and Electronic Documents Act	Partially compatible with GDPR	It is recognised as adequate for commercial data but has differences in legal regulation
New Zealand	New Zealand's Privacy Act	Recognised by the European Commission as a country with adequate protection	Complies with EU data protection standards
Brazil	General Data Protection Law	Largely consistent with GDPR	An analogue of GDPR, created to protect data in Brazil
South Korea	Personal Information Protection Act 2012	Compatible with GDPR after amendments	Recognised by the European Commission as a country with adequate data protection

Source: developed by the author based on Data privacy laws and regulations around the world (2024)

Data encryption in the cloud environment has become a cornerstone of cybersecurity in the face of the rapid growth of information volumes and an increase in the number of cyber threats. The age of digitalisation, when data becomes an essential asset, requires companies to provide reliable solutions to protect them. The future of encryption in the cloud promises to be dynamic and multifaceted, reflecting the latest trends in technology, regulation, and security approaches (Subbiah *et al.*, 2020). One of the most substantial areas is the use of quantum encryption. Quantum technologies based on the principles of quantum mechanics can provide a level of security that is inaccessible to traditional encryption methods. Quantum encryption allows creating systems capable of detecting data interception attempts, which makes it an ideal solution for protecting information in the cloud. Research in this area is actively developing, and perhaps it is more likely to see a wider application of quantum methods in cloud services, which will increase the level of data protection, especially in the face of increasing cyber threats.

Another important trend is adaptive encryption algorithms. Given that cyber threats are becoming more complex and diverse, adaptive algorithms that can dynamically change their parameters depending on conditions will gain popularity. Such systems can

automatically adjust the level of protection based on the type of data being processed or the threat level. This will not only increase security but also optimise performance, providing the necessary level of protection. Integration with artificial intelligence (AI) will also be an important area of encryption development in the cloud environment. AI and machine learning are already beginning to find applications in cybersecurity, and this area continues to develop (Shankar *et al.*, 2020). AI can help automate encryption and decryption processes and analyse and predict potential threats. AI-based systems will be able to detect anomalies and suspicious activities, which will increase the level of data protection and respond promptly to threats.

With the rise of cybersecurity threats, it can be expected that government agencies and regulators will continue to tighten data protection requirements. This will lead to the creation of new encryption standards and stricter requirements for companies using cloud solutions. Organisations will have to adapt to these changes, which will require substantial investments in technology and employee training (Srinivas *et al.*, 2019). The future of encryption will largely depend on the ability of companies to respond to changes in legislation in a timely manner and implement appropriate security measures. Thus, the future of encryption in the cloud environment is a complex combination of opportunities and challenges.

The development of quantum encryption, adaptive algorithms and integration with AI open up new horizons for improving data security. Nevertheless, companies must be prepared for the constant changes and challenges that will accompany this process. Maintaining a balance between security and data availability will be a critical factor in the successful implementation of encryption in the cloud in the future. In the context of digitalisation, encryption will remain an important tool for protecting both corporate and personal information, ensuring stability and trust in cloud services.

DISCUSSION

Data encryption is an integral element of modern digital security, and its importance is steadily growing against the background of increasing threats of information leaks and cyber-attacks. Every year, the volume of processed and stored data increases, which makes the need for reliable protection of personal and corporate information more urgent. D.B. Rawat *et al.* (2019) mentioned that data encryption plays an important role in ensuring cybersecurity and emphasises the need to use modern encryption algorithms. The authors discussed how the evolution of threats requires constant updating of encryption methods and recommendations on the choice of algorithms. The authors placed great emphasis on technological evolution and recommendations for choosing algorithms, whereas the current results focus more on regulatory aspects and key management.

In terms of goals, data encryption is aimed at protecting the confidentiality, integrity, and accessibility of information. It ensures that only authorised users can access the data and that the information has not been changed during the transfer process. A. Bhardwaj & S. Goundar (2019) noted that encryption in a cloud environment requires a balance between security and performance, and warned against blind trust in the built-in tools of providers. This is critically important in an environment where information is transmitted over open networks and can be intercepted by intruders. The results of this study emphasised the role of key management and regulations, while the author focused on possible vulnerabilities in data transmission networks.

There are two main encryption methods – symmetric and asymmetric. Each of them has its advantages and disadvantages, and the choice between them depends on the specific conditions of use. Symmetric encryption, based on the use of a single key for encryption and decryption, is characterised by high speed and efficiency. However, its main disadvantage is the need for reliable transmission of the secret key, which can become a vulnerability. In the context of asymmetric encryption, using a public and private key pair provides a high level of security, although it requires more computing resources and time for data processing. Q. Zhang (2021) discussed the importance of asymmetric encryption in securing transactions in e-business. He pointed to its high effectiveness in protecting sensitive data such as credit card numbers, while highlighting the challenges associated with key management. The author focused more on e-commerce and transaction security, whereas the current study analysed a wider range of encryption applications, including corporate data.

Within the modern digital space, companies face challenges related to key management and integration of various data protection methods. Key management is not only a technical task but also an important aspect of the organisational process that requires constant monitoring and revision. Secure key transfer between parties can be a substantial challenge, especially in large organisations with multiple users. Loss or compromise of a key can lead to loss of access to important information, which makes key management critically important.

Data encryption is also becoming necessary to comply with GDPR requirements, which introduces strict standards for the protection of personal information. M. Brodin (2019) considered the impact of regulations on the implementation of encryption in business processes. The author mentioned that compliance with GDPR and other regulations has become an important requirement for companies, which leads to the need to invest in encryption technologies. Unlike the results of this study, the author focused on the complexity of implementing encryption for small and medium-sized businesses.

M.N. Ramachandra *et al.* (2022) focused on performance issues related to encryption in cloud

environments. They discussed the trade-offs between security and performance and recommended optimising the encryption process to improve efficiency. Nevertheless, compliance with high security standards not only minimises the risks of violations but also increases customer trust, which is an important competitive advantage in the market. This study focuses more on key management, while the authors focus on optimising computing processes to improve performance.

The analysis showed that despite the advantages of encryption, there were many difficulties associated with its implementation in a cloud environment. For example, performance may be hampered by the computing resource requirements required to encrypt and decrypt data. M.N. Alenezi *et al.* (2020) emphasised that symmetric encryption is effective for large amounts of data, while asymmetric encryption ensures the security of key exchange. They focused on the need to integrate encryption into cybersecurity strategies. This study also recognises the effectiveness of symmetric encryption for large amounts of data and the importance of asymmetric encryption for secure key exchange. The integration of encryption into cloud solutions also requires a careful assessment of the dependence on cloud service providers.

The future of data encryption in cloud technology promises to be dynamic. The key areas of development may be quantum encryption and adaptive algorithms that can change their parameters depending on the threat level. These technologies can offer a higher level of information protection, which is especially important in the context of increasing cyber threats. S. Sonko *et al.* (2024) explored the future of encryption with a focus on quantum technologies. The authors discussed how quantum encryption can change the approach to data protection, providing a new level of security and resistance to cyber-attacks. Integrating AI into encryption processes can also improve responsiveness to potential threats by optimising encryption and decryption processes. In the current study, quantum technologies and AI are not the main focus, however, it can be agreed that this aspect is important for encryption.

Key management, regulatory compliance and the integration of new technologies will be vital factors determining the effectiveness of encryption in the future. It is important that organisations not only implement encryption as a technical process but also develop a culture of data security to protect their information and maintain user trust in a constantly changing digital landscape. H. Aldawood & G. Skinner (2019) emphasised the importance of building a culture of data security and employee training to minimise the risks of information leaks in organisations. The authors highlighted that employee training and the implementation of best practices in data management and encryption are necessary to reduce the risks of leaks. The results focus on encryption and key management technologies but it is worth considering the issue of human capital.

In the context of increasing threats to cybersecurity and the increasing volume of processed data, encryption has become an integral element of information protection at both the personal and corporate levels. The choice of encryption methods – symmetric or asymmetric – depends on the specifics of the application, the required level of security and available resources. Y. Dong *et al.* (2021) considered quantum encryption and adaptive algorithms as the future of data encryption, emphasising the importance of integrating AI to improve security and responsiveness to threats. The authors also discussed future technological innovations. They also recognised the prospects of quantum encryption and adaptive algorithms for the future of data protection and discussed future technological innovations. The current study also placed great emphasis on the challenges of current encryption in cloud environments, while the author discussed more about future technological innovations.

Key management is a critical task that requires special attention, as compromising a key can lead to loss of access to important information. In addition, the need to comply with regulatory requirements such as GDPR highlights the importance of integrating encryption into business processes. I. Issa *et al.* (2020) emphasised the importance of encryption for regulatory compliance, emphasising the need to regularly update key management processes to minimise the risks of leaks. An important aspect is the balance between security and performance, especially in cloud environments where high demands on computing resources can slow down data access. The current results also focused on the issues of balancing security and performance in cloud environments.

Thus, data encryption is not only a technical process but also a strategic element of cybersecurity, requiring an integrated approach to implementation and constant updating and new technologies. Organisations must implement encryption as a tool and develop a culture of data security, ensuring the protection of information and maintaining user trust.

CONCLUSIONS

This study analysed the importance of data encryption in the modern digital world and its role in ensuring information security. Every year, due to the growing volume of processed and stored data, the need to protect personal and confidential information is becoming more urgent. Encryption is the process of converting information into an unreadable format, which allows protecting it from unauthorised access. This technology is not only an important element of security but also meets the requirements of modern regulations such as GDPR.

The study showed that the main purpose of data encryption is to ensure the confidentiality, integrity, and accessibility of information. Encryption ensured that only authorised users could access the data, preventing

potential leaks and information theft. The use of encryption algorithms, such as symmetric and asymmetric encryption, allows effectively protecting of data, each of which has its own characteristics and security level.

Symmetric encryption, characterised by using the same key for encryption and decryption, stands out for its high speed and efficiency but requires reliable key transfer. Therewith, asymmetric encryption using a key pair (public and private) provided a higher level of security and solved the problem of secure key transfer but has its drawbacks in the form of slow operation and increased computing resources.

One of the critical challenges faced by companies is the management of encryption keys. Improper management can lead to data loss or compromise. Therefore, it is important to regularly update keys and apply comprehensive security measures, including digital signatures and secure data transfer protocols. GDPR has become an important step in the field of personal information protection, requiring companies to comply with strict security standards. This became a challenge for many organisations that had to adapt their business processes to new requirements. Compliance with these standards has increased customer confidence and strengthened the companies' position in the market.

In general, data encryption is a powerful tool to ensure the security of information in the digital world. Its proper implementation and the use of additional security measures will help prevent data leaks and increase user confidence in systems that work with confidential information. In the context of the rapid growth of data volumes and the increase in cyber threats, encryption remains an important aspect of cybersecurity that requires constant attention and adaptation.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abroshan, H. (2021). A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Computer Science and Applications*, 12(6). doi: 10.14569/IJACSA.2021.0120604.

[2] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs – pitfalls and ongoing issues. *Future Internet*, 11(3), article number 73. doi: 10.3390/fi11030073.

[3] Alenezi, M.N., Alabdulrazzaq, H.K., & Mohammad, N.Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, 12(2), 256-272. doi: 10.17762/ijcnis.v12i2.4698.

[4] Al-Shabi, M.A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications*, 9(3), 576-589. doi: 10.29322/IJSRP.9.03.2019.p8779.

[5] Amazon Web Services. (2024). Encrypting AWS services. In *AWS key management service* (pp. 1001-1031). Seattle: Amazon Web Services.

[6] Asghar, M.N., Kanwal, N., Lee, B., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual surveillance within the EU general data protection regulation: A technology perspective. *IEEE Access*, 7, 111709-111726. doi: 10.1109/ACCESS.2019.2934226.

[7] Azure encryption overview. (2024). Retrieved from https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview.

[8] Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cyber security and cloud performance. *Computer Fraud & Security*, 2019(2), 12-19. doi: 10.1016/S1361-3723(19)30020-X.

[9] Brodin, M. (2019). A framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research*, 4(2), 243-264. doi: 10.1007/s41125-019-00042-z.

[10] Calder, A., & Watkins, S. (2024). *IT governance – an international guide to data security and ISO27001/ISO27002*. London: IT Governance Publishing. doi: 10.2307/j.ctv336p2z9.

[11] Custers, B., Sears, A.M., Dechesne, F., Georgieva, I., Tani, T., & van der Hof, S. (2019). *EU personal data protection in policy and practice*. The Hague: TMC Asser Press. doi: 10.1007/978-94-6265-282-8.

[12] Data privacy laws and regulations around the world. (2024). Retrieved from https://securiti.ai/privacy-laws/.

[13] Dong, Y., Huang, X., Mei, Q., & Gan, Y. (2021). Self-adaptive image encryption algorithm based on quantum logistic map. *Security and Communication Networks*, 2021(1), article number 6674948. doi: 10.1155/2021/6674948.

[14] General Data Protection Regulation (GDPR). (2016). Retrieved from https://gdpr-info.eu/.

[15] Gui, Z., Paterson, K.G., & Patranabis, S. (2023). Rethinking searchable symmetric encryption. In *IEEE symposium on security and privacy* (pp. 1401-1418). San Francisco: Institute of Electrical and Electronics Engineers. doi: 10.1109/SP46215.2023.10179460.

[16] Issa, I., Wagner, A.B., & Kamath, S. (2020). An operational approach to information leakage. *IEEE Transactions on Information Theory*, 66(3), 1625-1657. doi: 10.1109/TIT.2019.2962804.

[17] Key purposes and algorithms. (2024). Retrieved from https://cloud.google.com/kms/docs/algorithms.

[18] Li, J., Huang, Y., Wei, Y., Lv, S., Liu, Z., Dong, C., & Lou, W. (2019). Searchable symmetric encryption with forward search privacy. *IEEE Transactions on Dependable and Secure Computing*, 18(1), 460-474. doi: 10.1109/TDSC.2019.2894411.
[19] Malvai, H., Kokoris-Kogias, L., Sonnino, A., Ghosh, E., Oztürk, E., Lewi, K., & Lawlor, S. (2023). Parakeet: Practical key transparency for end-to-end encrypted messaging. In *Network and Distributed System Security (NDSS) symposium 2023*. San Diego, CA: NDSS. doi: 10.14722/ndss.2023.24545.
[20] Marqas, R.B., Almufti, S.M., & Ihsan, R.R. (2020). Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. *Journal of Xi'an University of Architecture & Technology*, 12(3), 3110-3116. doi: 10.37896/JXAT12.03/262.
[21] Matulevičius, R., Tom, J., Kala, K., & Sing, E. (2020). A method for managing GDPR compliance in business processes. In N. Herbaut & M. La Rosa (Eds.), *Advanced information systems engineering* (pp. 100-112). Cham: Springer. doi: 10.1007/978-3-030-58135-0_9.
[22] Palit, T., Monrose, F., & Polychronakis, M. (2019). Mitigating data leakage by protecting memory-resident sensitive data. In D. Balenson (Ed.), *Proceedings of the 35th annual computer security applications conference* (pp. 598-611). New York: Association for Computing Machinery. doi: 10.1145/3359789.3359815.
[23] Rafique, A., Van Landuyt, D., Beni, E.H., Lagaisse, B., & Joosen, W. (2021). CryptDICE: Distributed data protection system for secure cloud data storage and computation. *Information Systems*, 96, article number 101671. doi: 10.1016/j.is.2020.101671.
[24] Ramachandra, M.N., Srinivasa Rao, M., Lai, W.C., Parameshachari, B.D., Ananda Babu, J., & Hemalatha, K.L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. *Big Data and Cognitive Computing*, 6(4), article number 101. doi: 10.3390/bdcc6040101.
[25] Rawat, D.B., Doku, R., & Garuba, M. (2019). Cybersecurity in Big Data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, 14(6), 2055-2072. doi: 10.1109/TSC.2019.2907247.
[26] Rudnytskyi, V., Korchenko, O., Lada, N., Ziubina, R., Wieclaw, L., & Hamera, L. (2022). Cryptographic encoding in modern symmetric and asymmetric encryption. *Procedia Computer Science*, 207, 54-63. doi: 10.1016/j.procs.2022.09.037.
[27] Sajay, K.R., Babu, S.S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*. doi: 10.1007/s12652-019-01403-1.
[28] Senthilkumar, R., & Geetha, B.G. (2020). Asymmetric Key Blum-Goldwasser Cryptography for cloud services communication security. *Journal of Internet Technology*, 21(4), 929-939. doi: 10.3966/160792642020072104003.
[29] Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A., & de Albuquerque, V.H. (2020). Adaptive optimal multi key based encryption for digital image security. *Concurrency and Computation: Practice and Experience*, 32(4), article number e5122. doi: 10.1002/cpe.5122.
[30] Shukla, D.K.R., Dwivedi, V.K., & Trivedi, M.C. (2021). Encryption algorithm in cloud computing. *Materials Today: Proceedings*, 37(2), 1869-1875. doi: 10.1016/j.matpr.2020.07.452.
[31] Sonko, S., Ibekwe, K.I., Ilojianya, V.I., Etukudoh, E.A., & Fabuyide, A. (2024). Quantum cryptography and US digital security: A comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. *Computer Science & IT Research Journal*, 5(2), 390-414. doi: 10.51594/csitrj.v5i2.790.
[32] Srinivas, J., Das, A.K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-188. doi: 10.1016/j.future.2018.09.063.
[33] Subbiah, S., Palaniappan, S., Ashokkumar, S., & BalaSundaram, A. (2020). A novel approach to view and modify data in cloud environment using attribute-based encryption. In G. Ranganathan, J. Chen & Á. Rocha (Eds.), *Inventive communication and computational technologies* (pp. 197-204). Singapore: Springer. doi: 10.1007/978-981-15-0146-3_20.
[34] Zeng, M., Zhang, K., Qian, H., Chen, X., & Chen, J. (2019). A searchable asymmetric encryption scheme with support for Boolean queries for cloud applications. *The Computer Journal*, 62(4), 563-578. doi: 10.1093/comjnl/bxy134.
[35] Zhang, Q. (2021). An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. In *2nd international conference on computing and data science* (pp. 616-622). Stanford: Institute of Electrical and Electronics Engineers. doi: 10.1109/CDS52072.2021.00111.

Шифрування даних як метод захисту персональних даних у хмарному середовищі

Самур Ахмадов
Аспірант
Азербайджанський технічний університет
AZ1073, просп. Гусейна Кавіда, 25, м. Баку, Азербайджан
https://orcid.org/0000-0003-0733-898X

Анотація. У контексті хмарних технологій шифрування відіграє ключову роль, оскільки дані постійно передаються мережею і зберігаються на віддалених серверах, що робить їх потенційною мішенню для кібератак. Мета дослідження полягала у всебічному аналізі методів шифрування даних як основного інструменту для захисту персональної інформації в хмарних сервісах. Розглянуто сучасні технології шифрування, включно із симетричним та асиметричним шифруванням, а також їхнє застосування в різних хмарних платформах. Проведено порівняльний аналіз цих методів з погляду їхньої ефективності, впливу на продуктивність систем і складності в реалізації. Важливим аспектом дослідження стало вивчення проблем, пов'язаних з управлінням ключами шифрування, включно з їхнім безпечним зберіганням і захистом від несанкціонованого доступу. У рамках дослідження також розглянуто приклади успішного впровадження шифрування на популярних хмарних платформах і способи забезпечення їхньої відповідності вимогам законодавства у сфері захисту персональних даних. Проаналізовано нормативні акти, що регулюють обробку та зберігання персональної інформації, та їхній вплив на вибір і реалізацію методів шифрування в хмарі. Результати дослідження показали, що шифрування залишається одним із найнадійніших способів захисту даних у хмарному середовищі, але для його ефективного застосування необхідний комплексний підхід. Оптимальний захист даних включає не тільки шифрування, а й управління ключами, регулярний моніторинг безпеки та навчання персоналу. Це допоможе мінімізувати ризики витоків даних і підвищити довіру користувачів до хмарних сервісів

Ключові слова: управління ключами; продуктивність систем; інформаційна безпека; витоки інформації; конфіденційність